Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

BSI-Veröffentlichungen zur Cyber-Sicherheit

EMPFEHLUNG: ANWENDER

Sichere Nutzung von Edge-Computing

1 Inhaltsverzeichnis

1 Inhaltsverzeichnis ... 3
2 Einleitung ... 5
3 Grundlagen von Edge Computing ... 9
3.1 Grundverständnis ... 9
3.2 Abgrenzungen ... 12
3.3 Rahmenbedingungen (Governance und Compliance) ... 12
4 Technologie ... 15
4.1 Infrastruktur ... 15
4.1.1 Edge (und Fog) Computing Modelle ... 15
4.2 Netztechnologien ... 18
4.2.1 Software Defined Networking (SDN) ... 18
4.2.2 Funknetze ... 19
4.3 Komponenten ... 20
4.3.1 Cloudlets ... 20
4.3.2 Integration in Netzkomponenten ... 21
4.3.3 Integration in Endgeräte ... 22
5 Exemplarische Use Cases ... 23
5.1 Einleitung ... 23
5.2 Use Case 1: IoT für Gesellschaft (Verkehrssteuerung/Smart City) ... 23
5.2.1 Definition ... 23
5.2.2 Relevante Gefährdungen ... 25
5.2.3 Angriffsszenario 1: Angriff auf die Verfügbarkeit ... 26
5.2.4 Angriffsszenario 2: Angriff auf die Vertraulichkeit und Integrität ... 28
5.3 Use Case 2: IoT für Industrie (Predictive Maintenance) ... 29
5.3.1 Definition ... 29
5.3.2 Relevante Gefährdungen ... 31
5.3.3 Angriffsszenario 1: Angriff durch einen Außentäter ... 32
5.3.4 Angriffsszenario 2: Angriff durch einen Innentäter ... 34
5.4 Use Case 3: Datenverarbeitung und Enterprise Security (Hochfrequenzhandel an der Börse) ... 35
5.4.1 Definition ... 35
5.4.2 Relevante Gefährdungen ... 36
5.4.3 Angriffsszenario 1: Angriff durch Außentäter über die Edge-Ebene ... 37
5.4.4 Angriffsszenario 2: Angriff durch Innentäter über die Edge-Ebene ... 38
6 Sicherheitsbetrachtungen für die praktische Umsetzung ... 40
6.1 Einleitung ... 40
6.2 Praxisleitfaden ... 41
6.2.1 Planung und Beschaffung (PB) ... 42

6.2.2 Einsatz (EZ) 45
6.2.3 Ende des Einsatzes (EX) 56
7 Anhang 1 Literaturverzeichnis 58
8 Anhang 2 Abbildungsverzeichnis 59

2 Einleitung

Edge Computing ist ein technologischer Trend, der sich zunehmend etabliert und in der Breite Anwendung findet. Mit dieser "Cyber-Sicherheitsempfehlung zur sicheren Nutzung von Edge Computing" beabsichtigt das BSI Handlungsempfehlungen zur bestmöglichen Absicherung dieser Technologie zur Verfügung zu stellen.

Folgende Grundbegriffe werden im Dokument verwendet und haben in diesem Zusammenhang die hier beschriebenen Bedeutungen:

Begriff	**Definition**
Bereitstellungsmodelle	Das Bereitstellungsmodell eines Cloud-Dienstes definiert, wo die IT-Infrastruktur zur Erbringung des Cloud-Dienstes verortet ist, und welche Cloud-Kunden gemeinsam Zugriff auf diese IT-Infrastruktur haben. Die am meisten verbreiteten Bereitstellungsmodelle sind dabei „public“, „private“, „hybrid“ und „multi“. Diese Modelle können in Ansätzen auch auf Edge Computing übertragen werden.
fixed Black Box-Modell	Als fixed Black Box bezeichnet man im Machine Learning-Kontext ein austrainiertes KI-Modell, bei dem die Ein- und Ausgabe bekannt sind, jedoch nur wenige bis keine Informationen über die inneren Abläufe des Modells vorliegen.
C-ITS	C-ITS ist die Abkürzung für “Cooperative Intelligent Transport Systems”, auch „Kooperative intelligente Verkehrssysteme“. Im Rahmen von C-ITS tauschen vernetzte Fahrzeuge und die Verkehrsinfrastruktur digitale Funknachrichten zum Verkehrsgeschehen und zum Fahrzeugzustand aus.
C-ITS-Station	Es handelt sich bei einer C-ITS-Station um eine Ansammlung von Hardware- und Software-Komponenten der Fahrzeuge oder Verkehrsinfrastruktur, welche den C-ITS-Dienst erbringen.
Cloud Computing	Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen („Cloud-Dienste“) erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der in diesem Rahmen angebotenen Cloud-Dienste umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Anwendungen [12].
Cloudlets	Ein Cloudlet ist ein Architekturelement, das aus der Konvergenz von mobilem Computing/IoT und Cloud Computing entsteht. Es entspricht der mittleren Schicht innerhalb einer dreischichtigen Hierarchie: Mobiles/IoT-Device - Cloudlet – Cloud [5].
Data Poisoning	Der Begriff "Data Poisoning" bezeichnet eine Klasse von Machine Learning-Angriffen, welche eine Manipulation des vom Machine Learning-Modells verwendeten Trainingsdatensatzes inkludieren
Dienste-Anbieter	Ein Dienste-Anbieter (auch „Cloud- oder Edge-Anbieter“) ist im Sinne des Cloud und Edge Computings ein Unternehmen oder eine Institution, in seltenen Fällen auch eine natürliche Person, welches bzw. welche einen Cloud- oder Edge-Dienst bereitstellt.
Dienste-Nutzer	Ein Dienste-Nutzer (auch „Cloud- oder Edge-Kunde“) ist im Sinne des Cloud oder Edge Computings ein Unternehmen oder eine Institution, in seltenen Fällen auch eine natürliche Person, das bzw. die mit dem Cloud- oder Edge-Anbieter zum Zwecke der Nutzung des Cloud- oder Edge-Dienstes in einer Geschäftsbeziehung steht.

Begriff	Definition
Edge Computing	Edge Computing ist serviceorientiertes Anbieten und Nutzen von verteilten Systemen zur Verarbeitung von Daten räumlich nah am Bedarf außerhalb einer Cloud
eMBB	Enhanced Mobile Broadband (eMBB) ist eine Funktion, die bei der Mobilfunktechnologie 5G eingeführt wurde, damit eine höhere Übertragungsgeschwindigkeit und Bandbreite zur Verfügung gestellt wird.
Evasion Attacks	Evasion Attacks sind eine Klasse von Machine Learning-Angriffen, welche eine Manipulation der Eingabedaten des Machine Learning-Modells inkludieren.
Fog Computing	Fog Computing ist serviceorientiertes Anbieten und Nutzen von verteilten Systemen zur Verarbeitung von Daten räumlich nah am Bedarf am Rande einer Cloud.
"hybrid" Cloud	„Hybride“ Clouds beschreiben ein Bereitstellungsmodell, bei welchem eigenständige Cloud-Infrastrukturen unterschiedlicher Bereitstellungsmodelle über standardisierte Schnittstellen miteinander verknüpft werden.
IaaS	IaaS ist die Abkürzung für „Infrastructure as a Service“. Beschrieben wird somit ein Servicemodell, bei welchem der Cloud-Anbieter dem Cloud-Kunden einen virtualisierten Zugriff auf IT-Ressourcen wie Server oder Datenspeicher bietet. Alle Abstraktionsebenen von der Virtualisierungsschicht aufwärts werden vom Cloud-Kunden betrieben, welcher seine eigenen Dienste auf den IT-Ressourcen aufbauen kann.
IAM-Maßnahmen	IAM ist die Abkürzung für „Identity and Access Management“. IAM-Maßnahmen umfassen Maßnahmen zum Authentifizieren und Autorisieren einzelner Benutzer.
ITaaS	ITaaS ist die Abkürzung für „IT as a Service“. Trotz der namentlichen Ähnlichkeit handelt es sich hierbei nicht um ein klassisches Cloud-Servicemodell im Sinne von IaaS, PaaS oder SaaS. Anbieter ermöglichen vielmehr den Edge Computing-Nutzern, einzelne "public" Cloud-Dienste On-Premises selbst zu hosten. Die entsprechende Hardware wird zum Standort des Nutzers geliefert und dort in die Infrastruktur integriert. Rackspace, Strom, Netzverbindungen und Kühlung werden hingegen vom Nutzer bereitgestellt.
Machine Learning	Durch Machine Learning lernen IT-Systeme mit Hilfe von Trainingsdaten (Erfahrungswerten) Probleme zu lösen. Hierbei wird keine statische Zuordnung von Eingangswerten zu Ausgangswerten übernommen, sondern Gesetzmäßigkeiten und Muster genutzt, so dass auch bei unbekannten Eingangswerten Antworten generiert werden können.
mMTC	Massive Machine Type Communication (mMTC) ist eine Funktion, die bei der Mobilfunktechnologie 5G eingeführt wurde, um Daten von einer sehr großen Zahl von Endgeräten (bspw. IoT-Geräte) auf sehr begrenztem Raum entgegenzunehmen und zu verarbeiten.
MEC	MEC ist die Abkürzung für "Multi-Access Edge Computing". Beschrieben wird eine durch ETSI standardisierte Form des Edge Computings, welche über ein Zugangsnetz, wie z.B. das RAN, realisiert werden kann. Cloud-Technologie kann somit direkt auf Netz-Ebene angewandt werden.
"multi" Clouds	„Multi“ Clouds beschreiben ein Bereitstellungsmodell, bei welchem verschiedene Cloud-Dienste von unterschiedlichen Cloud-Anbietern bezogen werden. Dies kann aus Redundanzgründen, aber auch aus Ergänzungsgründen initiiert werden.

Begriff	Definition
Network Function Virtualization (NFV)	Es handelt sich bei NFV um ein Abstraktionskonzept, bei dem Netzfunktionen von ursprünglich dedizierter und meist proprietärer Hardware entkoppelt werden. Diese Funktionen bzw. Services werden von Switches, Routern, Firewalls, Load Balancer, Content Delivery, Edge Security etc. durch virtuelle Appliances auf standardisierten Rechenknoten umgesetzt. Der wesentliche Unterschied zu SDN ist, dass SDN einen Fokus auf die Abstraktion des Netzes setzt, während NFV zur Abstraktion der Funktionen und Dienste dient
On-Premises	On-Premises bezeichnet klassische IT-Systeme und/oder -Infrastrukturen, die in den eigenen Räumlichkeiten betrieben werden.
PaaS	PaaS ist die Abkürzung für „Platform as a Service“. Beschrieben wird somit ein Servicemodell, bei welchem der Cloud- oder Edge-Anbieter dem Cloud- oder Edge-Kunden einen virtualisierten Zugriff auf komplette Entwicklungsumgebungen mit standardisierten Schnittstellen bietet. Alle Abstraktionsebenen von der Runtime aufwärts werden vom Cloud- oder Edge-Kunden betrieben, welcher seine eigenen Anwendungen auf der Plattform ausführen kann.
Predictive Maintenance	Der Begriff "Predictive Maintenance" bezeichnet die proaktive Wartung von Maschinen auf Basis zuvor erhobener Mess- und Produktionsdaten.
"private" Cloud	„Private“ Clouds beschreiben ein Bereitstellungsmodell, bei welchem nur der Cloud-Kunde über ein internes Netz Zugriff auf den Cloud-Dienst hat. „Private“ Clouds werden meist vom Cloud-Kunden oder einem Dienstleister (ausschließlich) für den Kunden betrieben.
"public" Cloud	„Public“ Clouds beschreiben ein Bereitstellungsmodell, bei welchem die Allgemeinheit über ein öffentlich zugängliches Netz Zugriff auf den Cloud-Dienst hat. „Public“ Clouds werden meist vom Cloud-Anbieter betrieben.
RAN	RAN ist die Abkürzung für "Radio Access Network", auch "Funkzugangsnetz". Beschrieben wird der Teil eines Mobilfunknetzes, der als Bindeglied zwischen den Endgeräten und dem Kernnetz fungiert.
Rand der Cloud	Der Rand der Cloud beschreibt in dieser Cybersicherheitsempfehlung eine von den anderen Cloud-Systemen separierte Verarbeitungsumgebung, die genutzt wird, um beispielsweise geographische Vorteile zu erhalten, eine hohe Rechenleistung zu erzielen oder Rechenaufgaben an einen physischen Anker zu binden. Sie wird schematisch meist der Cloud zugeordnet, kann aber auch außerhalb der Cloud liegen.
Roadside Stations	Roadside Stations bezeichnen C-ITS-Stationen, die nicht in Fahrzeugen verbaut sind, sondern als Verkehrsinfrastruktur-Komponenten, zum Beispiel am Straßenrand, aufgebaut werden.
Robustness oder Robustheit (im Kontext Machine Learning)	Die Robustheit eines Modells im Machine Learning Umfeld bezeichnet die Integrität der Funktionen unter dem Einfluss von Störfaktoren. Die Robustness eines Modells wird meist im Kontext von Angriffen verwendet, welche die Ausgabe des Modells manipulieren.
Resilience / Resilienz (im Kontext Machine Learning)	Die Resilienz eines Modells im Machine Learning Umfeld bezeichnet die Verfügbarkeit der Funktionen unter dem Einfluss von Störfaktoren. Die Resilienz eines Modells wird meist im Kontext von Angriffen verwendet, welche das Modell selbst manipulieren.
SaaS	SaaS ist die Abkürzung für „Software as a Service“. Beschrieben wird hiermit ein Servicemodell, bei welchem der Cloud- oder Edge-Anbieter dem Cloud- oder Edge-Kunden einen virtualisierten Zugriff auf Software-Anwendungen bietet. Alle Abstraktionsebenen werden vom Cloud- oder Edge-Anbieter betrieben, der Cloud- oder Edge-Kunde agiert in diesem Modell also als reiner Benutzer der Anwendung.

Begriff	Definition
SDN	SDN ist die Abkürzung für „Software Defined Networking“. Beschrieben wird ein Architekturansatz, bei welchem die Daten- und Steuerungsebene separiert werden. Die Steuerung erfolgt dabei softwaregesteuert und zentralisiert. Der wesentliche Unterschied zu NFV ist, dass SDN einen Fokus auf die Abstraktion des Netzes setzt, während NFV zur Abstraktion der Funktionen und Dienste dient.
Servicemodelle	Das Servicemodell eines Cloud- oder Edge-Dienstes definiert, welche Abstraktionsebenen der auf dem Cloud- oder Edge-Dienst aufbauenden Anwendung der Verantwortung des Cloud- oder Edge-Anbieters unterliegen, und welche der Verantwortung des Cloud- oder Edge-Kundens unterliegen (siehe Shared Responsibility). Die verbreitetsten Servicemodelle sind dabei IaaS, PaaS und SaaS.
Shared Responsibility	Shared Responsibility beschreibt ein integrales Sicherheitskonzept des Cloud Computings, nach dem die Verantwortung für die einzelnen Abstraktionsschichten einer Anwendung unter dem Cloud-Anbieter und dem Cloud-Kunden aufgeteilt werden. Die Partei, welche für eine spezifische Abstraktionsschicht verantwortlich ist, ist zu deren kontrollierter und sicherer Bereitstellung verpflichtet. Das Sicherheitskonzept kann auch auf Edge Computing übertragen werden.
Smart City	In einer Smart City wird intelligente Informations- und Kommunikationstechnologie verwendet, um Teilhabe und Lebensqualität zu erhöhen und eine ökonomisch, ökologisch und sozial nachhaltige Kommune zu schaffen.
uRLLC	Ultra Reliable Low Latency Communication (uRLLC) ist eine Funktion, die bei der Mobilfunktechnologie 5G eingeführt wurde, um schnelle Antwortzeiten für Anwendungen (Annäherung an Echtzeit) zu liefern.
V2X-Kommunikation	V2X ist die Abkürzung für „Vehicle-to-Everything“, auch „Fahrzeug-zu-X“. Der Begriff Fahrzeug-zu-X umfasst die Funk-Kommunikation von Fahrzeugen zur Verkehrsinfrastruktur, zu anderen Fahrzeugen sowie anderen Verkehrsteilnehmern.
Vendor Lock-In	Ein Vendor Lock-In im Sinne des Cloud- oder Edge Computings liegt vor, wenn der Wechsel von einem Cloud- oder Edge-Dienst zu einem äquivalenten anderen Cloud- oder Edge-Dienst mit so hohen Kosten verbunden ist, dass er für den Cloud- oder Edge-Kunden nicht möglich ist. Solche hohen Kosten entstehen meist aus starken Abhängigkeiten zu dem bisherigen Cloud- oder Edge-Anbieter, zum Beispiel aufgrund der Verwendung proprietärer Datenformate.
Verteilte Systeme	Verteilte Systeme bezeichnen im Sinne des Edge Computings eine in sich abgeschlossene Ansammlung von IT-Systemen, die betrieben werden, um die digitale Erfüllung einer Aufgabe dynamisch und skalierbar auszuführen.

3 Grundlagen von Edge Computing

In diesem Kapitel wird zunächst das aktuelle Grundverständnis des BSI zu Edge Computing beschrieben. Danach werden als Abgrenzung der thematische Schwerpunkt und dessen Grenzen für diese Cyber-Sicherheitsempfehlung erläutert. Die Rahmenbedingungen beschreiben, welche Vorschriften und Vorgaben grundsätzlich beim Einsatz von Edge Computing beachtet werden müssen. Diese sind gemeinsam mit dem Einsatzzweck und den technischen Gegebenheiten Grundlage für die später beschriebenen Sicherheitsempfehlungen und die Analyse der Gefährdungen und Risiken.

3.1 Grundverständnis

Cloud Computing ermöglicht es (auch "kleineren") Nutzern, bei relativ geringen Investitionskosten hoch spezialisierte Dienste in Form eines Mietmodells zu nutzen, z.B. KI-Anwendungen. Der Betrieb wird dabei an ein professionelles Angebot bzw. in zentralisierte Rechenzentren ausgelagert. Insbesondere wiederkehrende oder rechenintensive Aufgaben lassen sich durch Cloud-Angebote skalierbar und dynamisch nutzen. Cloud-Dienste werden aktuell entsprechend häufig genutzt, sei es als "public", "private", "hybrid", oder "multi" Cloud-Angebote. Es ist davon auszugehen, dass sich die Akzeptanz und Nutzung von Cloud Computing in der Zukunft noch weiter erhöhen wird.
Für einige Anwendungsszenarien sind Cloud-Dienste jedoch nur bedingt geeignet, beispielsweise für Echtzeitanwendungen oder für Anwendungen, bei denen hohe Datenvolumina für die Verarbeitung zum Verarbeitungsort und zurück transportiert werden müssen. Dies ist auf die vergleichsweise hohen Latenzen bzw. hohen Transitkosten zurückzuführen. Lösungen für solche Probleme oder auch zur Erfüllung von ortsabhängigen Compliance-Vorschriften bietet der Technologieansatz Edge Computing.

Es gibt verschiedene Anwendungsfälle, in denen Edge Computing-Technologie genutzt werden kann. Diese umfassen ein sehr weites Spektrum wie

- Industrial IoT
    - intelligente Aktoren und Sensoren
    - Distributed Control Systems (DCS)
    - Kameras
    - Augmented Reality (Bsp. visuelle Wartungsanleitungen)
- IoT für die Gesellschaft
    - Smartmeter
    - Landwirtschaftliche Maschinen
    - Medizinprodukte
    - Transportsysteme
    - Automotive
    - Smart Cities
    - Smart Borders
- Datenverarbeitung und Enterprise Security
    - Compliance-konforme Datenverarbeitung
    - (schnelle) Auslieferung von Webseiten (Content Delivery/Distribution Networks)
    - Sensoren in IT-Systemen/Netzkomponenten, beispielsweise Protokollierungsdatenanalyse oder DDoS-Mitigation, Malware-Detection/Prevention
    - Anwendungen mit sehr hohen Anforderungen an Rechenleistungen und Latenz
    - 5G (Multi Access Edge Computing (MEC))

Grundannahmen:

Im Fachdiskurs und in der Breite des Anwendungsspektrums ist der Begriff Edge Computing nicht eindeutig definiert. Da sehr unterschiedliche Use Cases unter dem Begriff Edge Computing zusammengefasst werden können, ist es auch nicht einfach, eine allgemeingültige Definition zu finden. Edge Computing ist aus Sicht des BSI eine Weiterentwicklung der 2017, 2018 durch NIST [2] und das Open Fog Consortium [3] als Quasi-Standard beschriebenen Technologie Fog Computing. Während Fog-Technologie noch als Teil der Cloud oder Ergänzung der Cloud quasi am Rande der Cloud angeboten wurde, rückte die Technologie unter der Bezeichnung Edge Computing im Laufe der letzten Jahre näher an die Endgeräte, deren Daten in den Komponenten verarbeitetet wurden.

Das BSI geht daher zur klaren Abgrenzung zunächst von folgenden Grundannahmen aus, welche im Kapitel 4 "Technologie" weiter in der Tiefe ausgeführt werden. In Kapitel 5 werden beispielhafte Anwendungsfälle betrachtet und die Grundannahmen in Kapitel 6 einem Praxischeck unterzogen.

Fog Computing *beschreibt serviceorientiertes Anbieten und Nutzen von verteilten Systemen zur Verarbeitung von Daten räumlich nah am Bedarf am Rande einer Cloud. Mit Fog Computing werden vergleichbar zu Cloud Computing Dienste aus den Bereichen SaaS, PaaS und IaaS angeboten. Der Unterschied zur Cloud ist, dass diese Dienste ortsgebunden angeboten werden, um Latenzen zu reduzieren oder andere geographische Vorteile wie die Einhaltung von Compliance-Vorschriften (wie beispielsweise Datenschutz) an diesem Ort zu ermöglichen.*

Verteilte Systeme *bedeuten hier eine in sich abgeschlossene Ansammlung von IT-Systemen (zur Bereitsstellung von Rechenleistung, Speicher, Netz, Managementfunktionen), die betrieben werden, um die digitale Erfüllung einer Aufgabe dynamisch und skalierbar auszuführen. Laut Definition Andrew S. Tanenbaum (emeritierter US-amerikanischer Professor für Informatik an der Freien Universität Amsterdam (Niederlande)) handelt es sich bei einem verteilten System um den Zusammenschluss unabhängiger Computer, die sich für den Benutzer als ein einziges System präsentieren [14].*

Mit ***Rand der Cloud*** *ist eine meist von den anderen Cloud-Systemen separierte Verarbeitungsumgebung gemeint, die genutzt wird, um beispielsweise geographische Vorteile zu erhalten, eine hohe Rechenleistung zu erzielen oder Rechenaufgaben an einen physischen Anker zu binden. Diese separierte Verarbeitungsumgebung kann Teil einer Cloud sein oder außerhalb der Cloud liegen, sie wird schematisch aber der Cloud zugeordnet.*

Edge Computing *ist bedarfsnahes, serviceorientiertes Anbieten und Nutzen von verteilten Systemen zur Verarbeitung von Daten außerhalb einer Cloud und räumlich nah am Bedarf. Mit Edge Computing werden vergleichbar zu Fog und Cloud Computing Dienste aus den Bereichen SaaS, PaaS und IaaS angeboten.*

In der Praxis wird der Begriff Fog Computing fast gar nicht mehr verwendet. Um eine anwendbare Verwendung des Begriffes bei der sicherheitstechnischen Bewertung der in der Praxis eingesetzten Komponenten zu ermöglichen, wird auch im BSI nur der Begriff Edge Computing verwendet. Hierbei muss unterschieden werden, ob die Technologie im Endgeräte-Netz eingesetzt wird, außerhalb des Endgeräte-Netzes oder direkt in der Netztechnologie wie bei 5G Multi-Access Edge Computing. Zur Differenzierung für die Sicherheitsbetrachtung, ob die Edge-Komponenten innerhalb des Endgeräte-Netzes oder außerhalb liegen, werden für diese Cyber-Sicherheitsempfehlung die Begriffe innere und äußere Edge-Ebene verwendet.

In der folgenden Abbildung wird schematisch dargestellt, wie Edge Computing mit Cloud-Systemen und Endgeräten verbunden ist.

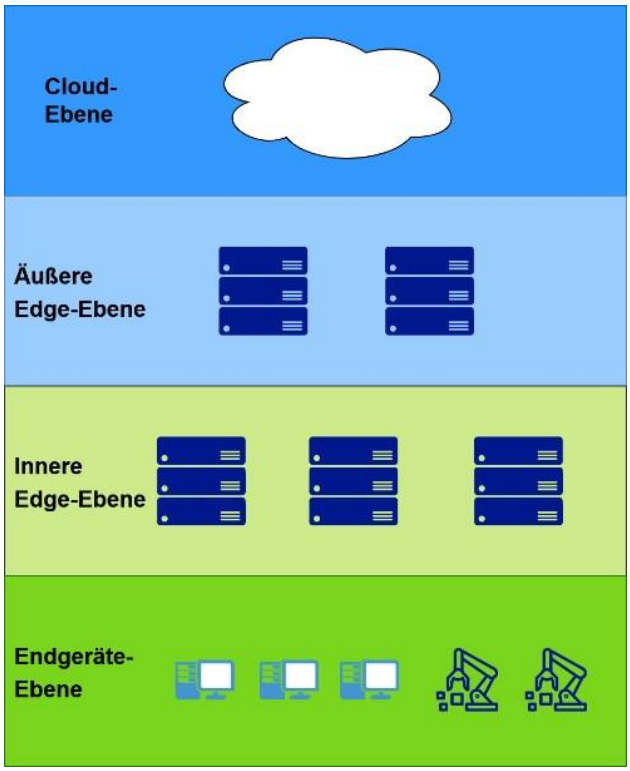

Abb. 1 Zusammenspiel zwischen Endgeräten, Edge Computing und Cloud Computing

Es wird an dieser Stelle auf eine detaillierte Beschreibung aller möglichen Komponenten verzichtet, da je nach Use Case unterschiedliche Komponenten und Zusammenstellungen verwendet werden. Es soll zunächst ein abstraktes Grundverständnis für die beteiligten Ebenen Cloud, Edge und Endgeräte hergestellt werden. In den folgenden Kapiteln wird detaillierter erläutert, welche Komponenten und Netztechnologien zum Einsatz kommen und wie unterschiedlich diese bei den verschiedenen Use Cases zum Einsatz kommen. Hier wird modellhaft von einer möglichen Abgrenzung zwischen den Ebenen ausgegangen. In praktischen Use Cases können sich diese Grenzen überschneiden.

In der untersten Ebene befinden sich die Endgeräte. Endgeräte können hier Kameras, Sensoren, Aktoren oder vergleichbar sein, welche Daten zur Verarbeitung anliefern oder die Ergebnisse aus der Verarbeitung entgegennehmen. Alternativ können Endgeräte auch größere Geräte sein, die wiederum Aktoren oder Sensoren unterschiedlicher Art beinhalten, wie beispielsweise Autos, landwirtschaftliche Geräte, Laptops, Tablets, Smartphones. Darüber hinaus gibt es Technologien, bei denen eine Verarbeitung bereits im Endgerät vollzogen wird und zwar in dem Maße, dass von einer Edge-Funktionalität ausgegangen werden kann. Je nach Vernetzungsgrad gibt es dann keine klare Abgrenzung mehr zwischen Endgeräte-Ebene und Edge-Ebene.

In der inneren Edge-Ebene, welche sich ebenso wie die Endgeräte im Endgerätenetz befinden, werden über verteilte Systeme dynamisch Edge-Dienste zur Verfügung gestellt, die eine schnelle und lokal sehr nahe Verarbeitung der Endgeräte-Daten erfordern. Dies können beispielsweise Sensordaten sein, die für eine zeitkritische Steuerung eines Aktors benötigt werden. Außerdem werden einzelne Daten zur langfristigen

Weiterverarbeitung an die äußere Edge- und/oder Cloud-Ebene weitergegeben, wo sie noch weiterverarbeitet werden. Diese Trennung zur Endgeräte-Ebene wird für die Sicherheitsbetrachtung notwendig, wenn beispielsweise fremdadministrierte Edge-Komponenten in das Endgeräte-Netz eingebracht werden. Hier wird eine netztechnische Separation innerhalb des Gesamtnetzes zwischen Endgeräten oder anderen Geräten des Anwenders und Edge-Komponenten notwendig.

In der äußeren Edge-Ebene werden über verteilte Systeme dynamisch Edge-Dienste zur Verfügung gestellt, die Berechnungen für die Cloud-Ebene vornehmen, um beispielsweise Daten für die dortige Verarbeitung zu reduzieren oder ortsabhängige Aufgaben für die untere Edge- und Endgeräte-Ebene zu übernehmen. Da sich diese Edge-Komponenten außerhalb des Endgerätenetzes und der Cloud befinden, wird auch hier modellhaft eine von den anderen Ebenen separierte Ebene eingefügt, um eine methodische Sicherheitsbetrachtung zu ermöglichen.
In der Cloud-Ebene werden in Rechenzentren Cloud-Dienste dynamisch und skalierbar zur Verfügung gestellt, die direkt oder über Edge-Komponenten der inneren oder äußeren Edge-Ebene von Nutzern eingesetzt werden können.

3.2 Abgrenzungen

Edge Computing baut auf vielen bereits ausführlich sicherheitstechnisch betrachteten Technologien und Anwendungen auf. Diese werden in dieser Cyber-Sicherheitsempfehlung nicht neu behandelt. Es wird für deren Einzelabsicherung auf die entsprechenden Cyber-Sicherheitsempfehlungen und Vorgaben verwiesen. Diese Cyber-Sicherheitsempfehlung beschäftigt sich mit den neuen Gefährdungen, die durch den Zusammenschluss der miteinander vernetzten Systeme und Ebenen und dem teilweise außergewöhnlichen Einsatzort in den verschiedenen Use Cases zu Stande kommen.

Laut den Grundannahmen zu Edge Computing in Kapitel 3.1 wird von "Berechnungen in verteilten Systemen" gesprochen. Dies bedeutet im Kontext dieses Dokumentes, wenn eine Berechnung auf einem Server oder dem Endgerät selbst durchgeführt wird, auch wenn diese sehr komplex ist, liegt hier nicht automatisch Edge Computing vor. Wenn dagegen dynamisch und skalierbar Ressourcen (wie Rechenleistung oder Speicher) durch einen Anbieter bereitgestellt werden, um beispielsweise Daten von Endgeräten bzw. anderen Edge- oder Cloud-Systemen zu verarbeiten, spricht man von Edge Computing. Dynamisch und skalierbar sind Merkmale für die bedarfsgerechte Bereitstellung der benötigten Ressourcen.

3.3 Rahmenbedingungen (Governance und Compliance)

Bei Edge Computing müssen verschiedene Compliance- und Governance-Vorgaben beachtet werden. Bei Compliance geht es um die Beachtung der gesetzlichen Rahmenbedingungen. Governance-Vorgaben beschreiben Unternehmens- oder Institutions-spezifische und strategische Regeln. Die Governance-Vorgaben beinhalten teilweise auch Regeln, wie spezifische Richtlinien umgesetzt werden. Es ist wichtig, zu Compliance- und Governance-Vorgaben Anforderungen abzuleiten, diese umzusetzen und kontinuierlich die Einhaltung zu überwachen. In diesem Abschnitt werden hierzu allgemeingültige Vorgaben angesprochen, die für alle Use Cases gelten sollen. Use Case-bezogene Vorgaben müssen je nach Unternehmensvorgaben, Einsatzgebiet und Branche ergänzt werden. Da für Edge Computing Cloud-Technologie zum Einsatz kommt, gelten grundlegend die gleichen Vorgaben wie im Cloud-Bereich.

Vergleichbar zum Cloud Computing ist es eine strategische Entscheidung, Edge Computing einzusetzen. Deshalb ist das Vorhandensein einer Strategie für die Nutzung von Edge-Technologie von zentraler Bedeutung. Diese Strategie sollte auch die Grundlage für die Wahl eines geeigneten Dienstes und/oder Anbieters sein. Es ist darauf zu achten, dass das Angebot zur eigenen IT passt und mit dem eigenen Schutzbedarf, Sicherheitsniveau und an die Institution oder das Unternehmen gerichteten Anforderungen an Compliance und Governance kompatibel ist.

Die Nutzung externer Dienste macht ein Unternehmen oder eine Institution immer mindestens teilweise von den jeweiligen Anbietern abhängig. Hier ist im Speziellen auf die Shared Responsibility hinzuweisen, bei der sowohl der Nutzer als auch der Anbieter Beiträge zur IT-Sicherheit leisten müssen. Die Institution

muss darauf achten, ausreichend Kontrolle über die ausgelagerten Geschäftsprozesse, Daten und deren Sicherheit zu behalten. Besonders wichtig sind hierbei auch (georedundante) Backups und Backupverträge. Hierbei sollten für jeden Teilabschnitt der Nutzung der Dienste (Auswahl, Beschaffung, Betrieb und Aussonderung) Vorkehrungen getroffen werden.

Bei der Auswahl sollte darauf geachtet werden, dass einige Dienste von internationalen Anbietern mit Anschluss an deren Cloud-Systeme angeboten werden und somit unterschiedlichen nationalen Gesetzgebungen unterliegen können. Aus diesem Grund müssen die rechtlichen Rahmenbedingungen wie Datenschutz, Informationspflichten, Insolvenzrecht, Haftung oder Informationszugriff für Dritte beachtet und mit den eigenen Vorgaben abgeglichen werden. Hierbei müssen beispielsweise Gesetze wie die DSGVO oder das IT-Sicherheitsgesetz eingehalten werden.

Für Beschaffung und Betrieb sind die vertraglichen Regelungen mit Anbietern entscheidend, da auch hier Sicherheitsprobleme auftreten können. Verantwortungsbereiche, Aufgaben, Leistungsparameter und Aufwände sollten genau und unmissverständlich beschrieben werden. Im Speziellen ist auf vertragliche Regelungen bezüglich Drittanbieter zu achten. Anbieter nutzen häufig die Dienste Dritter und sollten diese Abhängigkeiten offenlegen. Um die Möglichkeiten und Auswirkungen von Supply-Chain-Angriffen zu verringern, können durch so genannte Software Bill of Materials (SBOM) bzw. Hardware Bill of Materials (HBOM) Inventarlisten mit Angaben zur Version und zum Patchstand erstellt werden, so dass bei Bekanntwerden von Schwachstellen, schneller Mitigationsmaßnahmen eingeleitet werden können. Das BSI hat zu SBOM eine Technische Richtlinie [11] herausgegeben. Über NIS2 wird spätestens im Herbst 2024 die Umsetzung von diesbezüglichen Vorgaben für einige Unternehmen verpflichtend, bei entsprechenden nationalen Vorgaben schon früher. Sollte eine Edge-Komponente in Kritischen Infrastrukturen eingesetzt werden, dann muss auch hier darauf geachtet werden, dass die Verantwortung und die damit verbundenen gesetzlichen Pflichten weiterhin beim Betreiber der Kritischen Infrastruktur und nicht beim Anbieter der Edge-Komponente liegen und die entsprechenden Vorgaben eingehalten werden.

Es sollten immer Vorkehrungen für das Ende der Nutzung oder einen Wechsel zu einem anderen Anbieter getroffen werden. Gerade in kritischen Situationen, wie der Insolvenz oder dem Verkauf des Anbieters oder dem Auftreten von schwerwiegenden Sicherheitsbedenken, können ohne eine genaue vertragliche Regelung und ausreichende Vorkehrungen große Sicherheitsprobleme und Schäden entstehen. Hier ist auch explizit auf eine genau geregelte Datenlöschung nach Vertragsende zu achten. Ein Ausstieg oder Wechsel wird durch kompatible Dateiformate und ein separates Backup bei einem anderen Anbieter erleichtert. Bei einigen Uses Cases könnte dies den Austausch der kompletten Hardware beinhalten.

Da Edge Computing auf Cloud-Technologie basiert, gelten allgemein für die grundlegenden Aspekte auch hier die Standards, die sich auf Cloud-Sicherheit oder allgemeine IT-Sicherheit beziehen. Beispielhaft seien hier der Cloud Computing Compliance Criteria Catalogue (C5) oder der IT-Grundschutz des BSI, die relevanten Aspekte der ISO/IEC 27000-Reihe, oder die Cloud Controls Matrix der Cloud Security Alliance genannt.

Der C5 des BSI ist ein Kriterienkatalog an die Informationssicherheit für Cloud-Dienste. Die darin enthaltenen Kriterien sind aus bereits etablierten Standards abgeleitet. Ziel ist die transparente Darstellung der Informationssicherheit eines Dienstes auf Basis einer standardisierten Prüfung. Diese kann im Rahmen einer eigenen Risikoanalyse verwendet werden. Auch Compliance und Data Governance werden dabei durch die Kriterien abgedeckt. So werden beispielsweise Angaben zur Verfügbarkeit und Störungsbeseitigung, zu den eingesetzten Subdienstleistern, zur geografischen Lage der Rechenzentren und zum Umgang mit Ermittlungsanfragen staatlicher Stellen gefordert.

Der IT-Grundschutz ist ein Standard zum Aufbau eines Informationssicherheitsmanagementsystems (ISMS) und betrachtet einen ganzheitlichen Ansatz zur Informationssicherheit. Hiermit wird ein systematisches Vorgehen ermöglicht, um notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen. In den BSI-Standards werden hierzu Vorgehensweisen beschrieben. Im IT-Grundschutz-Kompendium sind mit den Bausteinen konkrete Anforderungen enthalten. Auf Cloud-Sicherheit wird im Speziellen im Grundschutz-Baustein "OPS.2.2 Cloud-Nutzung" eingegangen. Für grundsätzliche Aspekte können die Vorgaben auch auf Edge Computing übertragen werden.

Des Weiteren unterliegen KRITIS-Unternehmen, die Cloud- oder Edge-Dienste nutzen, weiteren Vorgaben für die IT-Sicherheit. So müssen sie beispielsweise die Einhaltung von IT-Sicherheit nach dem Stand der Technik regelmäßig gegenüber dem BSI nachweisen und sich an Branchenspezifische Sicherheitsstandards (B3S) halten.

4 Technologie

In diesem Kapitel wird beschrieben, welche Technologie für Edge Computing allgemein zum Einsatz kommt. Dies variiert von Use Case zu Use Case stark.
Überall gleich sind allerdings eine grundlegende Infrastruktur, die Komponenten und die verbindenden Netze, die in diesem Kapitel beschrieben werden. Es wird dafür auf bekannte Modelle wie vom NIST und dem Open Fog Consortium eingegangen und daraus ein Modell für die BSI-Arbeit abgeleitet. Auch die bei Edge Computing verwendeten Komponenten und Netztechnologien unterliegen anderen Anforderungen als in einem klassischen Umfeld und werden daher hier im Kapitel kurz für das allgemeine Verständnis erläutert.

4.1 Infrastruktur

Infrastrukturen, wie sie beim Edge Computing verwendet werden, können, je nach Anwendungsdomäne bzw. Anwendungsfall sehr unterschiedlich ausfallen. In der Regel handelt es sich jedoch technisch um ein logisch-hierarchisches Modell aus Rechen-, Netz-, Verwaltungs- und Speicher-Ressourcen, welche sowohl lokal als auch verteilt und in Clustern vernetzt zusammenwirken. Die Komponenten arbeiten mehr oder weniger direkt bzw. abstrakt mit den Daten der Daten-erzeugenden Komponenten und delegieren ihre Ausgaben jeweils bei Bedarf weiter an eine andere Komponente oder legen Daten für die Weiterverarbeitung in Cloud-Systemen ab.
In diesem Unterkapitel wird die für Edge Computing verwendete Infrastruktur modellhaft erläutert. Es wird eine grundlegende Infrastruktur beschrieben, die ganz oder teilweise in den verschiedenen Use Cases verwendet wird. Es werden alle beteiligten Komponenten und Netzverbindungen auf einem abstrakten Level angedeutet, um das Zusammenspiel zu veranschaulichen.

4.1.1 Edge (und Fog) Computing Modelle

Für einige Anwendungsszenarien sind die Möglichkeiten von reinen Cloud-Diensten zwar reizvoll, die Latenzen für den Anwendungszweck jedoch zu hoch. Auch führen in einigen Fällen Sicherheits- oder Datenschutzvorgaben dazu, dass "public" Cloud-Dienste zwar eine Lösung für das fachliche Problem sein könnten, aber nicht in der angebotenen Form genutzt werden können. Aus diesem Grund wurden bereits 2017, 2018 Dienste aus dem eigentlichen Cloud-Verbund ausgegliedert und unter dem Namen Fog Computing angeboten. Weiterentwicklungen, die immer näher an den "Edge" der Endgeräte heranwanderten, wurden dann später mit Edge Computing bezeichnet. Zum Zeitpunkt der Veröffentlichung der Cyber-Sicherheitsempfehlung wurde meistens nur noch von Edge Computing gesprochen.

4.1.1.1 Fog Computing-Modelle

Viele Veröffentlichungen zum Thema Edge oder Fog Computing beziehen sich auf das "Fog Computing Conceptual Model" von 2018 vom NIST. Die dort verwendete Struktur ist am leichtesten in Abb. 2 erkennbar, welche insbesondere die Heterogenität der unterschiedlichen Komponenten über die verschiedenen Abstraktionsschichten in einer Edge- oder Fog-Infrastruktur abbildet:

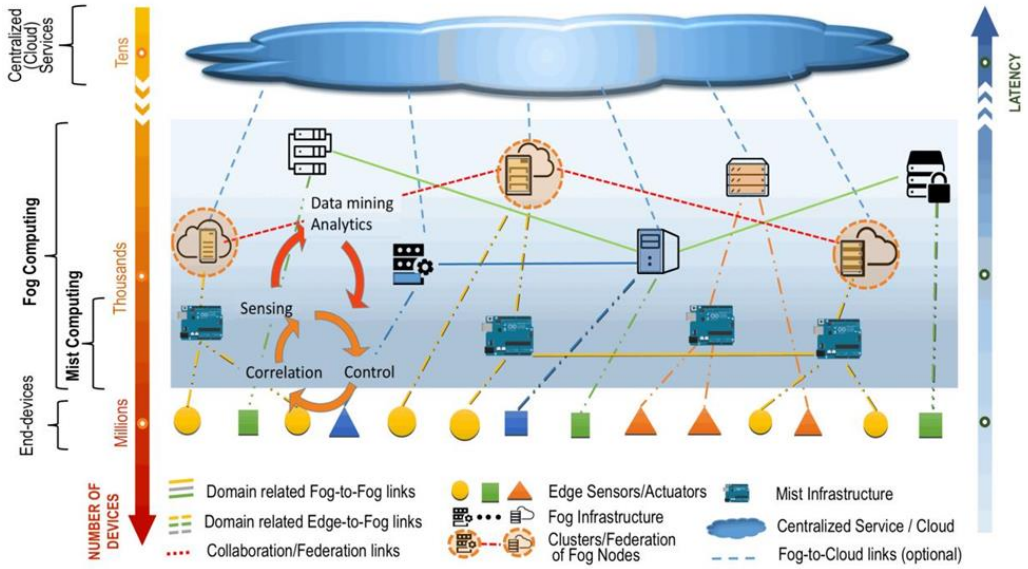

Abb. 2 NIST-Modell Fog Computing [2]

Die Abbildung zeigt parallel zu ihren y-Achsen den Abstraktionsgrad bzw. die hierarchische Ebene, auf der eine Komponente arbeitet. Wie in hierarchischen Systemen i.d.R. üblich, steigt mit der Entfernung zur Informations- bzw. Datenquelle auch der Grad der Abstraktion bzw. Aggregation. Analog dazu nimmt die Anzahl der Akteure ab, während die Antwortzeit steigt. Komponenten in den seinerzeit genannten Fog-Systemen werden i.d.R. mit steigendem Abstraktionsgrad smarter und übernehmen komplexere, rechenintensivere Aufgaben.

Die Grafik skizziert die unterschiedlichen Komponenten und deren Kommunikationsverbindungen untereinander. Die geometrischen Formen am unteren Ende der Grafik stellen dabei die verschiedenen Sensoren und Aktoren der Endgeräte dar. Ihre Anzahl kann im Millionenbereich liegen. In vielen Anwendungsfällen ist es erforderlich, dass die Auswertung von Sensordaten zur Steuerung von Aktoren in annähernder Echtzeit als Regelkreis erfolgt. Entsprechend hoch sind dann die Anforderungen an die Latenz. Regelkreise sind in der Grafik in logischer Sensor-Aktor-Nähe dargestellt. Die Server bzw. Steuerchips können sich dabei aber auch im selben Endgerät wie die Sensoren befinden. Um komplexere bzw. Endgeräte- oder Gruppen-übergreifende Aufgaben zu übernehmen, die immer noch relativ zeitkritisch sind, kommen die höheren Fog-Ebenen zum Einsatz. Diese können bereits Cloud Computing-ähnliche Servicemodelle wie IaaS, PaaS, SaaS etc. anbieten. Es entsteht je funktionale Anforderung an ein System eine Delegationskette. Am oberen Ende dieser Kette stehen ggf. Mini-Rechenzentren, "Private" und "Community" Clouds und schließlich auch eine Integration in Public Cloud-Dienste, die z.B. für weniger zeitkritische statistische Auswertungen des Gesamtsystems oder für die Archivierung von Daten eingesetzt werden können.

Eine weitere wichtige Arbeit bezüglich Fog Computing kommt vom Open Fog Consortium, welches bereits 2017 in seinem Grundmodell eine vereinfachte Darstellung gewählt hat, mit der die hierarchischen Aspekte besser erkennbar sind und damit als Grundlage für die weiteren Betrachtungen in dieser Cyber-Sicherheitsempfehlung dienen. Die vollständige Arbeit kann auf den Webseiten des Open Fog Consortiums [3] eingesehen werden.

4.1.1.2 Edge Computing-Modell

Mit der Weiterentwicklung von Cloud-Technologie und damit einhergehend der Netztechnologien, die im Kapitel 4.2 Netztechnologien ausführlicher beschrieben werden, wanderte die neue Technologie in die Endgerätenetze und wurde mehr und mehr auf spezifische Endgeräteszenarien ausgerichtet. Für die Arbeit im BSI wurden daher die bereits etablierten Modelle für Fog Computing als Grundlage genommen und um die innere Edge-Ebene im Endgerätenetz erweitert, wie in der Einleitung schon beschrieben und in Abb. 1 dargestellt.

In der Praxis werden nicht in allen Szenarien alle 4 Ebenen eingesetzt. Es gibt Szenarien, bei denen Edge-Komponenten nur auf der inneren Edge-Ebene oder nur auf der äußeren Edge-Ebene mit und ohne Cloud eingesetzt werden. Die einzige Konstante in allen Szenarien ist die Endgeräteebene. Da die Vielfalt schwer zu kategorisieren ist, soll an dieser Stelle ein Modell beschrieben werden, auf dessen Basis klarere Diskussionen zu Gefährdungen, Risiken und Sicherheitsempfehlungen durchgeführt werden können. Auch wird die Komplexität für das bessere Verständnis reduziert.

In Abb. 3 sind die 4 Ebenen aus Abb. 1 des zweiten Kapitels wieder aufgenommen und modellhaft mit Komponenten und Netzverbindungen dargestellt worden, die in den nächsten Unterkapiteln weiter erläutert werden. An dieser Stelle soll für das bessere Verständnis zunächst ein Gesamtbild über die Infrastruktur hergestellt werden.

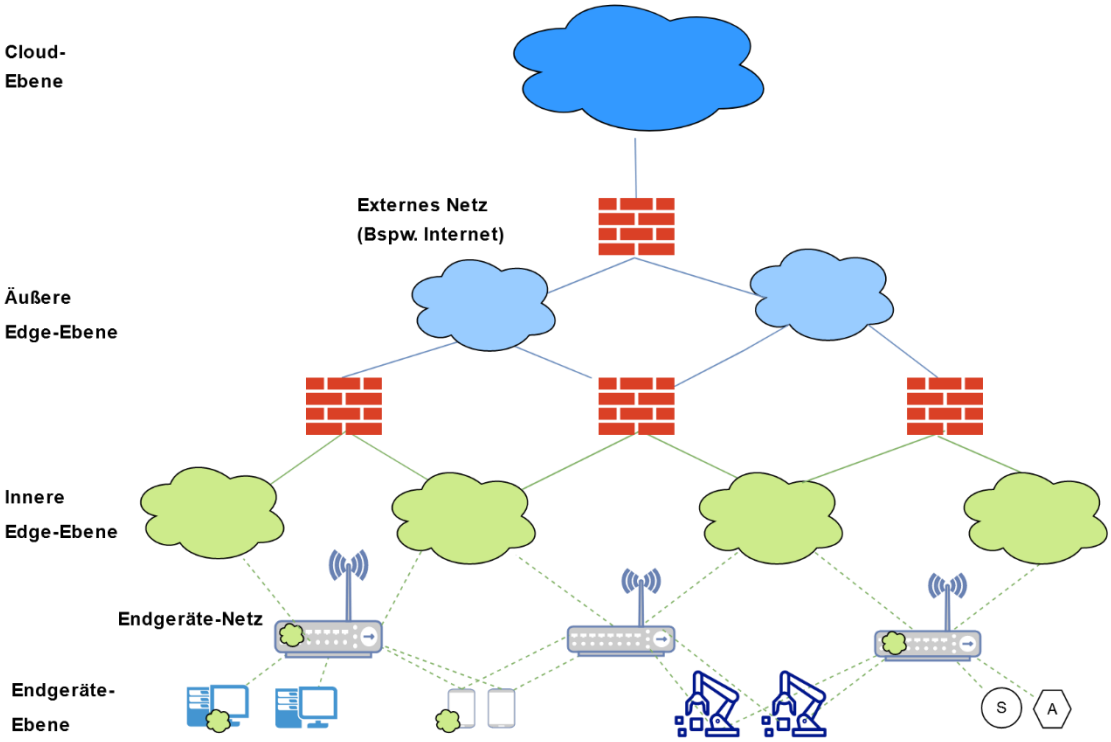

Abb. 3 Edge Computing-Modell für die BSI Arbeit

Auf der Cloud-Ebene werden eine große Menge Ressourcen (Rechenleistung, Verwaltung, virtuelle Netze, virtuelle Hardware, Verwaltungsfunktionen) zur Verfügung gestellt, die den Eindruck erwecken, die Ressourcen wären unbegrenzt verfügbar, wenn nur das ausreichende Geld investiert werden würde.

Auf der äußeren Edge-Ebene sind kleinere Wolken (hellblau eingefärbt) mit jeweils einer stärker begrenzten Anzahl von Ressourcen verfügbar. Dadurch, dass mehrere dieser kleineren Wolken, so genannte Cloudlets, verfügbar sind, kann in Summe wieder der Eindruck endloser Ressourcen entstehen. Die einzelnen Cloudlets sind aber ortsgebunden und können damit Anforderungen bzgl. Datenschutz, Sicherheit und Latenz an ihrem Standort besser erfüllen.

Die Cloudlets in der inneren Edge-Ebene, die hier grün eingefärbt sind, enthalten ähnlich wie die Cloudlets der äußeren Edge-Ebene eine begrenzte Anzahl von Ressourcen für die Bedienung anwendungsbezogener

Dienste, auch hier mit dem Ziel geringere Latenzen oder Sicherheitsfunktionen zur Verfügung zu stellen. Diese Cloudlets sind noch näher am Endgerät und befinden sich direkt im Endgerätenetz.

Zusätzlich gibt es Möglichkeiten die Technologie in Endgeräte oder Netzkomponenten unterzubringen, was weiter unten erläutert wird und hier im Bild schon angedeutet wird.

4.2 Netztechnologien

Wie im vorherigen Kapitel beschrieben, baut Edge-Technologie auf Cloud-Technologie und Virtualisierung auf. Das bedeutet, dass auch an die Netze dieselben Anforderungen wie an Cloud-Technik gestellt werden. Damit virtuelle Maschinen oder Container dynamisch zwischen Ressourcen verschoben werden können, um eine höhere Skalierbarkeit zu erreichen, müssen auch die Netze dynamisch und flexibel sein. Dies erreicht man meist durch virtuelle Netze und mobile Netze (Funktechnologien). Da diese Technologien vorwiegend eingesetzt werden und spezielle Eigenschaften mitbringen, die für Edge Computing Vorteile mitbringen, werden diese hier im Kapitel beschrieben. Eine physische Verbindung von einem Aktor oder Sensor zu einer Edge-Komponente, um eine schnellere Verbindung herzustellen wird in der Praxis eine Rolle spielen, diese wird aber nicht näher erläutert, da hierzu keine Technologie eingesetzt wird, die Edge-spezifische Vorteile mit sich bringt. Für das Verständnis der Kommunikationswege und die diesbezüglichen Herausforderungen bei der Absicherung werden die bei Edge Computing verwendeten Technologien hier kurz beschrieben. Für tiefer gehende Informationen wird auf die entsprechenden Referate des BSI und die dort aktuellen Veröffentlichungen verwiesen.

4.2.1 Software Defined Networking (SDN)

SDN wird in Edge Computing integriert, um die Vorteile von SDN und insbesondere die Optimierung hinsichtlich Netzeffizienz auszunutzen [6]. Durch den Einsatz von SDN profitiert die Gesamtarchitektur von der hierdurch möglichen einfachen Verwaltung und der niedrigen Latenz sowie Bandbreitennutzung, was die Echtzeitfähigkeit von Edge-Komponenten steigert [6][7].

Grundsätzlich beschreibt SDN einen neuen, innovativen Architekturansatz, der die Vereinfachung der Netzverwaltung und -analyse sowie eine Effizienzsteigerung bei flexibler Anpassung der IT-Infrastruktur ermöglicht. Dies wird durch die Trennung von Daten- und Steuerungsebene und gleichzeitiger Zentralisierung der Steuerung mittels Software erreicht. Praktisch werden die Separation und Zentralisierung der Steuerungsebene in Form von einem oder mehreren redundanten SDN-Controllern umgesetzt. Einen weiteren Vorteil stellt die Möglichkeit zur Umsetzung einer feingranularen Zugriffskontrolle dar, die durch die Programmierbarkeit der Netzstruktur entsteht. Dabei werden Netzgeräte, die die Funktion der Datenweiterleitung implementieren, als Netzknoten bzw. Netzelement bezeichnet. Dies gilt sowohl in klassischen als auch in SDN-Umgebungen. Die Netzgeräte werden in der reinen SDN-Lehre zu simplen Paketweiterleitungsgeräten und verfügen somit über keinerlei "Intelligenz". Die Verwaltung dieser erfolgt über APIs.

In IoT-Anwendungen können riesige Mengen an Datenströmen (z.B. von Telemetrie und Sensoren) entstehen und auch aggregierte Datenmengen (z.B. Fernüberwachung) von Edge-Komponenten können folglich das Transportnetz überlasten. Die SDN-Steuerungsebene in der Cloud oder Cloud-ähnlichen Systemen ermöglicht hierzu die Einbindung einer komplexen Verkehrskontrolle sowie Ressourcenverwaltung bzw. -zuweisung und kann daher zu einer verbesserten Lastverteilung beitragen. Durch die Kombination von Edge Computing mit SDN wird die Verteilung des Datenflusses an den jeweiligen Edge-Komponenten geregelt, wobei Pakete auf Basis von QoS-Spezifikationen klassifiziert und priorisiert werden können [6]. Mittels SDN und Network Functions Virtualization (NFV) werden IoT-Netze kosteneffizient virtualisiert, woraufhin die automatischen Datenflussumleitungen, einfachen Neukonfigurationen von Geräten und Bandbreitenzuweisungen sowie die zentrale Verwaltung von Sensoren, IoT-Gateways oder weiteren Geräten möglich sind [8]. Hierbei wird außerdem eine automatische Bereitstellung von Komponenten und benötigten Ressourcen inkl. Sicherheitsauthentifizierung sowie automatisierte Remote-Updates unterstützt [8]. SDN kann in Edge und Cloud Computing-Umgebungen zudem zu einer größeren Netztransparenz beitragen, da eine automatische Überwachung und Erkennung

von Sicherheitsbedrohungen sowie Anwendung von Sicherheitsrichtlinien und feingranularer Zugriffskontrolle erfolgt [8]. Für eine effiziente Verteilung von IoT-Analytik und Netzressourcennutzung ist jedoch eine genaue und umfassende Abstimmung von IoT-Plattform, SDN-Netz und Cloud-, Edge-Infrastruktur erforderlich [7].

4.2.2 Funknetze

Wie weiter oben schon beschrieben, wird bei Edge Computing mit verteilten Systemen gearbeitet, bei denen der Aufbau mit kabelgebundenen Netzen schwerer umzusetzen ist. Als Übertragungstechnik werden daher je nach Anwendungsfall meist unterschiedliche Funktechnologien eingesetzt.

4.2.2.1 WLAN

Unter dem Begriff Wireless Local Area Networks (WLAN) werden drahtlose Netze zusammengefasst, die in lokalen Umgebungen aufgebaut werden können. Die meisten WLAN-Komponenten basieren auf dem Standard IEEE 802.11 und seinen Ergänzungen, auf deren Basis das Hersteller-Konsortium „Wi-Fi Alliance“ mit „Wi-Fi“ einen Industriestandard geschaffen hat. Im Wi-Fi-Standard wird mit einem Gütesiegel bestätigt, dass ein Gerät gewisse Interoperabilitäts- und Konformitätstests bestanden hat. Für den Datenaustausch können zwischen Endgeräten Ad-Hoc-Verbindungen aufgebaut oder zwischen einem zentralen Zugangspunkt, dem Access Point, und verschiedenen Endgeräten etabliert werden.

Um niedrige Latenzen und die Möglichkeit der Übertragung großer Datenmengen zu realisieren, kommen bei der Übertragung für Edge Computing WLAN-Technologien ab Wi-Fi 5 in Frage, da ab Wi-Fi 5 die technischen Voraussetzungen für die Anforderungen an Edge Computing gegeben sind.

Wi-Fi 5 liefert Geschwindigkeiten von bis zu 7 GBit/s und Wi-Fi 6 bis zu 10 GBit/s und es werden immer weiter verbesserte Signalmodulationsverfahren wie OFDMA-Verfahren (Orthogonal Frequency Division Multiple Access) genutzt, die für eine bessere Ausnutzung der Funkkanäle sorgen, wodurch Nutzer an die Anforderungen für Echtzeitanwendungen herankommen, welche für viele IoT-Anwendungen benötigt werden. Die breiteren Kanäle erlauben den Transport größerer Datenmengen, die auch bei IoT-Anwendungen schnell anfallen. Auch der Datendurchsatz wurde in jeder Generation verbessert, ebenso, wie weitere Maßnahmen gegen Störanfälligkeit hinzugefügt wurden. Insbesondere eine geringe Störanfälligkeit ist für schnelle und gesicherte Reaktionen auf Sensorereignisse beim Edge Computing wichtig.

4.2.2.2 Mobilfunktechnologien

Mobilfunktechnologien wurden ursprünglich entwickelt, um Sprachübertragung mobil zu machen. Ab der Entwicklung von GSM-Standards (2G) war die Möglichkeit gegeben, Sprache auch digital zu übertragen. Mit jeder neuen standardisierten Generation kamen Möglichkeiten hinzu, weitere Informationen mit der Sprache zu übertragen, so dass bei 3G (UMTS) neben der Nutzung von Textnachrichten auch die Übertragung von Bilddaten (MMS) zu ermöglichen und bei 4G (LTE) war es möglich, Filme über Mobilfunk zu streamen.

Ab 5G haben Mobilfunktechnologien die Möglichkeiten der nichtsprachgebundenen Informationsverarbeitung und -Weiterleitung so erweitert, dass sie insbesondere für Edge Computing Use Cases eine Rolle spielen.

Eine Besonderheit von Mobilfunktechnologien ab der 5. Generation ist die Möglichkeit Netz-Slicing zu nutzen. Hier werden über SDN-Technologie verschiedene Netzebenen (Slices) aufgespannt, die softwaretechnisch voneinander isoliert sind. Hierdurch können Managementebene von der Datenebene getrennt werden, aber auch Security Slices oder für Kunden, die höhere Preise zahlen, priorisierte Slices mit beispielsweise schnelleren Übertragungsraten zur Verfügung gestellt werden. Da dies durch Software Defined Networks durchgeführt wird, können die Slices dynamisch und skalierbar, wie für Cloud- und Edge-Technologien benötigt, aufgespannt werden.

Funktionen wie Enhanced Mobile Broadband (eMBB) sollen eine höhere Übertragungsgeschwindigkeit und Bandbreite zur Verfügung stellen. Mit Funktionen wie Massive Machine Type Communication (mMTC)

sollen hier Möglichkeiten geschaffen werden, Daten von einer sehr großen Anzahl von Endgeräten (bspw. IoT-Geräte) auf begrenztem Raum entgegenzunehmen und zu verarbeiten. Funktionen wie Ultra Reliable Low Latency Communication (uRLLC) sollen eine schnelle Antwortzeit (nahezu Echtzeit) für Anwendungen auf Anfragen liefern. Im Bereich Edge Computing werden Funktionen wie eMBB, mMTC und uRLLC teilweise gleichzeitig benötigt. Mit 5G ist dies zum Zeitpunkt der Erstellung der Texte noch nicht möglich und 6G befindet sich noch in der Spezifizierungsphase. Dennoch sind die Funktionen für einige Use Cases auch einzeln hilfreich und, sofern vorhanden, können diese schon eingesetzt werden.

4.2.2.3 Bluetooth

Einige Endgeräte im IoT-Bereich haben nur Bluetooth als Verbindungsmöglichkeit integriert. Da wir in dieser Cyber-Sicherheitsempfehlung jedoch nur die Edge Computing-Komponenten betrachten, gehen wir davon aus, dass das Signal vor der Übernahme in Edge Computing in andere Formate umgewandelt wurde. Gefährdungen, die durch die Bluetooth-Nutzung in den Endgeräten entstehen, werden an anderer Stelle im BSI betrachtet.

4.3 Komponenten

Edge-Komponenten können unterschiedlich realisiert werden. Sie können in Endgeräte integriert oder als aktive Komponenten zu passiven Geräten hinzugefügt werden. Sie können auch als eigenständige Komponente realisiert werden, die aus mehreren Systemen zusammengesetzt ist, oder auf Netzebene in Netzkomponenten integriert werden. Im Folgenden werden unterschiedliche Formen beschrieben. Die Formen können beliebig kombiniert werden, teilweise treten sie auch einzeln auf. Die Kombination der Edge-Komponenten hängt stark vom Use Case ab. Aufgrund der Vielzahl der möglichen Use Cases wird im Folgenden eine abstrakte Darstellung gewählt. In den Use Case-spezifischen Beschreibungen in Kapitel 5 kann das Zusammenspiel anwendungsbezogen genauer betrachtet und analysiert werden. Zum besseren Verständnis werden für die unterschiedlichen Komponententypen einige zum Zeitpunkt der Erstveröffentlichung aktuelle Beispiele hinzugefügt. Absicht der Cyber-Sicherheitsempfehlung ist an dieser Stelle nicht, alle technischen Möglichkeiten vollständig zu beschreiben. Ziel ist vielmehr, ein Grundverständnis zu erlangen, das es ermöglicht, im weiteren Verlauf Gefährdungen und Risiken zu analysieren und entsprechende Sicherheitsempfehlungen dazu auszusprechen.

4.3.1 Cloudlets

Die Hauptfunktionalität von Edge Computing findet sich in Systemgruppen wieder, die aus mehreren verteilten Systemen zusammengesetzt sind und Cloud-ähnliche Dienste zur Verfügung stellen. Wir sprechen in diesem Zusammenhang von einer Edge-Komponente, wobei die Edge-Komponenten selbst meist wieder aus dem Zusammenschluss mehrerer Systeme bestehen. Oft wird eine solche Gruppe auch allgemein als Cloudlet bezeichnet.

Das Carnegie Mellon Software Engineering Institute [5] hat folgende Definition veröffentlicht, welche als früheste Nennung des Begriffes Cloudlet gilt: "A cloudlet is a new architectural element that arises from the convergence of mobile computing / IoT and cloud computing. It represents the middle tier of a 3-tier hierarchy: mobile or IoT device --- cloudlet --- cloud. A cloudlet can be viewed as a "data center in a box" whose goal is to "bring the cloud closer".

Ein Cloudlet kann reine Software sein (beispielsweise aus Openstack, Proxmox oder vergleichbar) oder als komplettes Bundle mit Hardware von einem Anbieter ausgeliefert werden. Mit einem Cloudlet wird eine Umgebung aufgebaut, mit der Servicemodelle wie IaaS, PaaS und SaaS angeboten und/oder genutzt werden können.

Ein Cloudlet wird wie eine Cloud über definierte Schnittstellen angesprochen und bietet skalierbar und dynamisch Dienste ähnlich wie die Cloud, aber ortsabhängig, an. Wie in Abb. 4 dargestellt, können hier Ressourcen wie beispielsweise Rechenleistung, Speicher oder Serverless Functions über Anwendungen für externe Aufgaben genutzt werden. Managementfunktionen sind zur Automatisierung, Absicherung, Verwaltung und Protokollierung ebenso enthalten wie physische und virtuelle Netzkomponenten. Die

Schnittstellen können unterschiedlicher Natur sein. Es können Funkschnittstellen sein, über die Chips, die an Endgeräte angeheftet werden, ausgelesen werden, oder gesendete Daten entgegennehmen. Ebenso gibt es Softwareschnittstellen, die herstellerspezifisch sind. Weit verbreitet sind hier Schnittstellen, die über Browser oder Konsolenprogramme bedient werden können. Einige Komponenten bringen sogar eigene Anwendungen mit, die auf Endgeräten installiert werden müssen. Auf Netzebene können Schnittstellen gebraucht werden, die die Zusammenarbeit mit Edge-Systemen auf Netzebene wie MEC (Multi-Access Edge Computing), welches weiter unten beschrieben wird, ermöglichen.

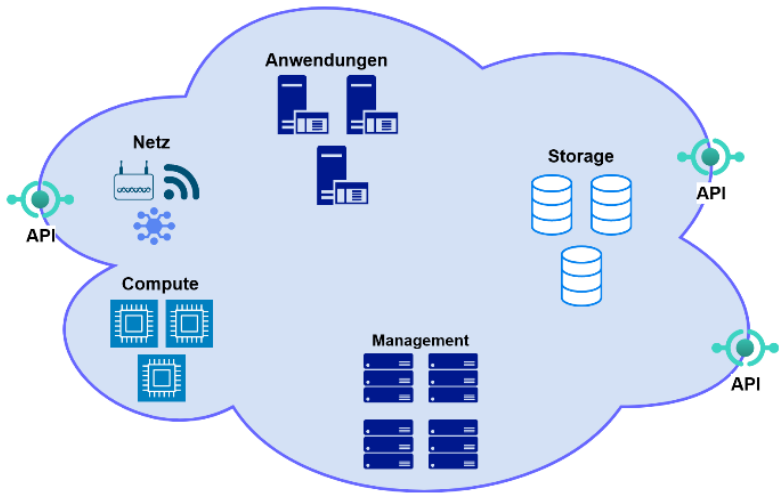

Abb. 4 Modellhafter Aufbau eines Cloudlets im angepassten Modell für die BSI Arbeit

4.3.1.1 ITaaS

ITaaS (IT as a Service) ist ein Beispiel für Cloudlets. Anbieter ermöglichen den Edge Computing-Nutzern mit ITaaS, einzelne Public Cloud-Dienste On-Premises selbst zu hosten.

Dabei wird die entsprechende Hardware zum Standort des Nutzers geliefert und dort in die Infrastruktur integriert. Dabei werden Rackspace, Strom, Netzverbindungen und Kühlung vom Nutzer bereitgestellt. Auf den Komponenten kann eine Auswahl von identischen Cloud-Diensten zur Nutzung von Rechenleistung, Speicher, Schnittstellen, etc. wie in einem Rechenzentrum des Anbieters genutzt werden. Die Konfiguration und Überwachung der Dienste ist meistens nahtlos in die Nutzersysteme integriert. Die Wartung der Hardware wird vom Anbieter übernommen. Die Kommunikationsverbindung zu einem Rechenzentrum des Anbieters erfolgt meist abgesichert über dedizierte, verschlüsselte VPN-Verbindungen oder vergleichbarem.
Im Edge-Umfeld können diese Lösungen eingesetzt werden, um zeitkritische Berechnungen nahe am Endgerät durchzuführen und damit Latenzen zu anderen Komponenten zu reduzieren, ohne dabei auf Cloud-Dienste verzichten zu müssen.

Eine wie oben beschriebene ITaaS-Komponente kann Teil eines "Cloudlets" im Architekturmodell einer Edge-Infrastruktur sein.

4.3.2 Integration in Netzkomponenten

Hauptsächlich sind Ziele von Edge Computing, Latenzen zu verringern oder große Datenmengen zu übertragen. Hierfür ist von großer Bedeutung, dass bei der Übertragung der Daten zwischen den einzelnen Systemen keine Verzögerungen aufkommen. Aus diesem Grund können über Technologien wie SDN und 5G Funktionen in die Netzebene hinein gezogen werden.

4.3.2.1 Multi-Access Edge Computing (MEC)

MEC ist ein Beispiel, wie Edge-Funktionalität direkt in die Netzebene integriert werden kann. MEC wurde für 5G von ETSI [4] standardisiert. Der genaue Aufbau und die Schnittstellen können in den einzelnen Spezifikationen nachgelesen werden. Mit MEC können Content Provider Anwendungsentwicklern direkt auf Netzebene die Möglichkeit anbieten, Cloud-Technologie anzuwenden, wodurch die Latenz deutlich herabgesetzt und bei Bedarf auch eine große Bandbreite zur Verfügung gestellt werden kann. Anbieter bekommen so die Möglichkeit, MEC Server in die Basisstationen zu integrieren, um ihr Radio Access Network (RAN) ausgewählten Teilnehmern zu öffnen, damit diese Anwendungen und Dienste flexibel und skalierbar anbieten können.

4.3.3 Integration in Endgeräte

Ebenso wie die Edge-Funktionalität über Netzkomponenten zur Verfügung gestellt werden kann, kann die Integration auch in Endgeräte erfolgen. Auch hier erreicht man mit einigen Zusatzkomponenten den Effekt von verteilten Systemen. Die komplette Funktionalität ist selten in den Endgeräten untergebracht, häufiger sind hier eher kleinere Endgerät-spezifische Vorberechnungen zu finden, die auf Cloudlets dann weiter zusammengeführt werden. Bei Bestandserfassungen können sogar passive Gegenstände wie Waren mit Funkchips ausgestattet sein, die Informationen zum Gegenstand wie Seriennummer, Haltbarkeit oder ähnlichem enthalten und abgefragt werden können.

5 Exemplarische Use Cases

5.1 Einleitung

In diesem Kapitel werden exemplarisch drei Use Cases beschrieben, die das in den vorherigen Kapiteln beschriebene Modell verdeutlichen sollen. Wie in der Einleitung erläutert, gibt es eine große Bandbreite an Möglichkeiten, Edge Computing einzusetzen. Um die unterschiedlichen Möglichkeiten der Anwendung des Modells in den verschiedenen Use Cases aufzuzeigen, werden aus den Gebieten "IoT für die Gesellschaft" (Use Case 1), "Industrial IoT" (Use Case 2) und "Datenverarbeitung und Enterprise Security" (Use Case 3) Szenarien beschrieben, die so auch in der Praxis umgesetzt sein könnten.

Die Ausarbeitung der unterschiedlichen Use Cases folgt dabei einer einheitlichen Struktur. Die Sachverhalte, welche den einzelnen Use Cases als Thema dienen, werden zunächst im Rahmen einer grundsätzlichen Definition vorgestellt. Zur besseren Veranschaulichung des Sachverhalts wird die allgemeine Erklärung durch konkrete Beispiel-Szenarien ergänzt. Anhand dieses Szenarios werden in Anlehnung an den IT-Grundschutz elementare Gefährdungen vorgestellt, von welchen die einzelnen Ebenen des Edge-Modells in diesem Szenario betroffen sein können. In einem nächsten Schritt wird veranschaulicht, wie die einzelnen Gefährdungen sich von einem Angreifer zu einem Angriffspfad verknüpfen lassen. Abschließend werden Handlungsempfehlungen zur Vermeidung einer solchen Verknüpfung präsentiert, sowie eine Einschätzung des verbleibenden Restrisikos nach Umsetzung der Handlungsempfehlungen gegeben. Bei den relevanten Gefährdungen und Handlungsempfehlungen wird an dieser Stelle bewusst nur mit "können", "sollten" und "könnten" gearbeitet, da es sich um fiktive Szenarien handelt. Ähnliche Szenarien in der Praxis müssen ausführlich analysiert und betrachtet werden. Hierzu soll der Praxisleitfaden, der in Kapitel 6 vorgestellt wird, Hilfestellung leisten.

Die Beschreibung der Use Cases soll hier allein dem besseren Verständnis der Technologie dienen. Die Use Cases sind rein fiktiv. Sie wurden so ausgewählt, dass sie ein breites Spektrum an möglichen Angriffen und Anwendungsgebieten darstellen und leicht verständlich sind. Die Texte, insbesondere die Beschreibung der Gefährdungen und Handlungsempfehlungen, haben an dieser Stelle daher bewusst keinen Anspruch auf Vollständigkeit. Es soll zunächst eine Grundlage geschaffen werden, wie das Modell angewendet wird. In der Praxis gibt es oft keine klare physische Trennung der Endgeräte- und Edge-Ebenen, wie das in den letzten Kapiteln im Modell beschrieben wurde. Logisch kann die Einteilung in Ebenen trotzdem auch weiter betrachtet werden, wenn sie physisch in ein und demselben Gerät liegen. Die getrennte Betrachtung der logischen Ebenen soll dazu dienen, die Komplexität der Technologien strukturiert erfassbar zu machen. Bei starken Überschneidungen der Ebenen auf physischer Seite wird dies im nachfolgenden Text zum besseren Verständnis beschrieben.

5.2 Use Case 1: IoT für Gesellschaft (Verkehrssteuerung/Smart City)

5.2.1 Definition

In diesem Use Case wird das Szenario aus dem Bereich Smart City an dem Beispiel einer auf Edge-Technologie basierenden Verkehrssteuerung betrachtet.

Ziel einer IoT-basierten Verkehrssteuerung ist es, den Verkehrsfluss zu optimieren. So können beispielsweise Staus vermieden und Einsatzfahrzeugen eine möglichst optimale Route, z. B. durch gezielte Ampelschaltungen, ermöglicht werden. Hierfür wird eine Vielzahl an Datenquellen genutzt, um ein möglichst genaues Bild der aktuellen Verkehrslage und des Verkehrsflusses zu erhalten. Diese Datenquellen können aus Sensoren an einer Straße selbst, wie Kameras, Bewegungsmelder oder Kontaktschleifen in der Fahrbahn, sowie aus Daten von Dritten, wie Verkehrsdaten aus den Systemen von modernen Autos (Fahrzeug-zu-X-Kommunikation), intelligenten Verkehrssystemen oder von Navigationsdiensten, bestehen. Eine mögliche Verwertung dieser Daten könnte sich wie folgt gestalten:

Die Daten der verschiedenen Quellen werden auf Komponenten der inneren Edge-Ebene (beispielsweise Roadside Stations) aggregiert, zur Weiterverarbeitung vorbereitet (bspw. Auswertung von Kamerabildern mit automatischen Fahrzeugerkennungen) und eine erste Zusammenfassung der Verkehrslage erstellt. Anschließend wird der hierbei neu entstandene Datensatz an die äußere Edge-Ebene weitergeleitet. Auf dieser werden die Datensätze verschiedener Standorte der inneren Edge-Ebene (beispielsweise einzelne Straßen oder Stadtviertel) gesammelt und ein Gesamtbild erstellt. Ebenso werden die Daten an die Cloud-Ebene weitergeleitet. Dort werden sie stochastisch ausgewertet, um eine dynamische Kapazitätsplanung zu ermöglichen. So können mit den Daten über einen größeren Zeitraum (z.B. ein Jahr) gewisse Erfahrungswerte über Einflüsse wie Datum, Uhrzeit, Wochentage, Feiertage, Großereignisse, Wetterlage, etc. gesammelt und entsprechende Vorhersagen über zukünftige Verkehrslagen erstellt werden. Durch den ständigen Zufluss von weiteren Datensätzen, können diese Erfahrungswerte kontinuierlich verbessert und neue Szenarien (extreme Wetterlagen, sich stetig verändernde Gewohnheiten durch z. B. allgemein verstärktes Arbeiten im Homeoffice oder stärkerer Pendelverkehr zum Beginn oder am Ende von Wochenenden) und Änderungen (neue oder veränderte Straßenführung, Bau oder Abriss von Einkaufszentren, etc.) berücksichtigt werden. Der aktuelle Stand dieser Erfahrungswerte wird in regelmäßigen Abständen zur äußeren Edge-Ebene gespiegelt und dort für Vorhersagen über den Verkehrsfluss berücksichtigt.

Auch gibt es Modelle, die Veränderungen des Verkehrsflusses durch gezielte Eingriffe (wie Ampelschaltungen, Tempolimits, etc.) simulieren. Diese werden in der Cloud ebenfalls durch die gelieferten Datensätze stetig verbessert und angepasst und in regelmäßigen Abständen in der aktuellen Version an die äußere Edge-Ebene zur Verwendung weitergegeben.

Aus den gesammelten und verarbeiteten aktuellen Daten, sowie den Erfahrungswerten und Modellen der Cloud-Ebene, kann nun ein Gesamtbild der Verkehrslage und eine Prognose für den weiteren Verkehrsverlauf erstellt werden. Basierend hierauf können Verkehrsoptimierungen berechnet und an die entsprechenden Aktoren zur Umsetzung weitergegeben werden. Solche Aktoren sind bspw.:

- Ampeln (Rot- und Grünphasen verlängern/verkürzen)
- Anzeigetafeln und elektronische Verkehrsschilder (Anzeige von Informationen, Warnungen, Tempolimits, Umleitungen, Freigabe von (Stand-)Spuren))
- Bereitstellung der Informationen an Radiostationen für Staumeldungen und (Warn-)Hinweise
- Bereitstellung der Informationen über APIs oder Funk an KFZ-Radios, Navigationssysteme, Apps, etc.
- Meldungen von Störungen (ausgefallene Ampeln, Staus, Unfälle) an Einsatzzentralen
- Bereitstellung von optimalen (und bspw. durch spezielle Ampelschaltungen vorbereitete) Routen an Einsatzkräfte

Durch einen Abgleich der Vorhersagen und eingeleiteten Maßnahmen mit dem anschließenden Ergebnis auf der Straße, können auf der äußeren Edge- und Cloud-Ebene die Modelle weiter angepasst werden. Insgesamt entsteht so ein sich kontinuierlich verbessernder und anpassender Kreislauf für Verkehrsvorhersagen und Optimierungen.

Als Beispiel für diesen Use Case wird eine fiktive Großstadt mit 300.000 Einwohnern betrachtet, die für ihre Verkehrsregelung ein wie oben beschriebenes Edge- und Cloud-System einsetzen möchte. Vor der Einführung wird eine Risikoanalyse durchgeführt.

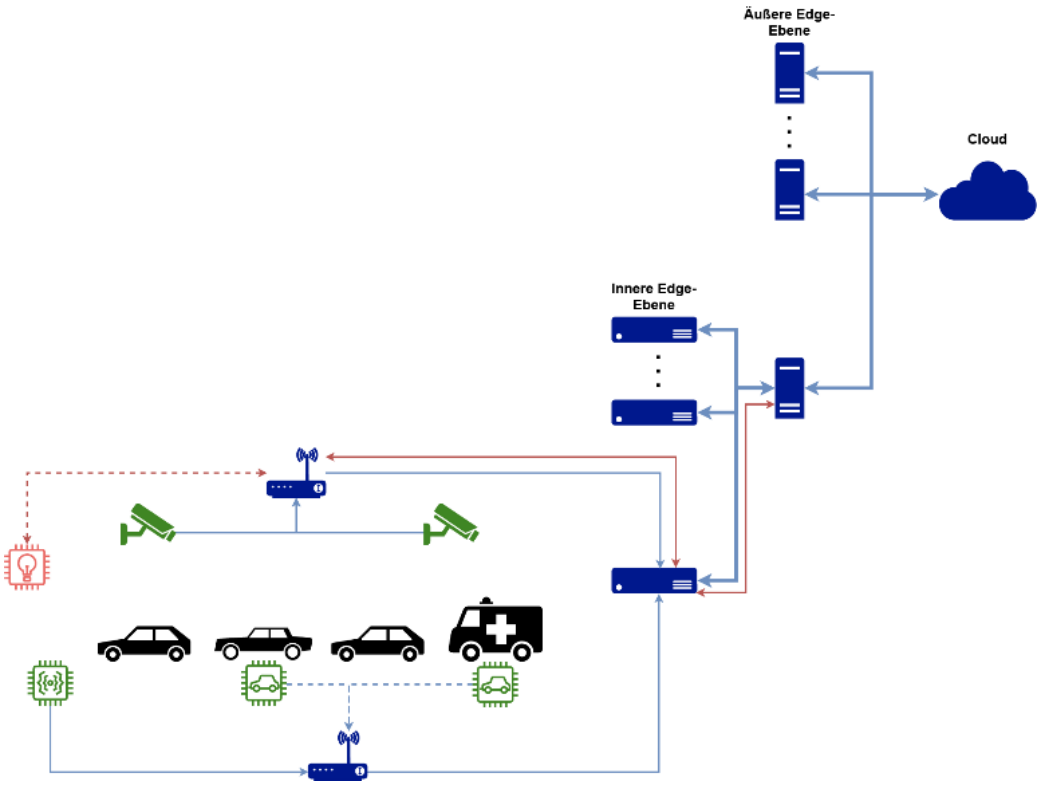

Abb. 5 IoT-basierte Verkehrsregulierung

Diese Grafik (Abb.5) gibt eine grobe Übersicht über einen exemplarischen Aufbau der IoT-basierten Verkehrsregulierung und den darin verwendeten Komponenten der inneren und äußeren Edge-Ebene sowie Cloud-Diensten. Auf einer Straße werden von verschiedenen Sensoren (grün) Daten gesammelt und an die Edge-Ebene (V2X-Nachrichten) weitergesendet, wo sie verarbeitet werden. Jede Komponente der inneren Edge-Ebene sendet wiederum ihre Daten an die äußere Edge-Ebene, wo sie weiterarbeitet und Entscheidungen getroffen werden. Die Komponente der inneren Edge-Ebene sendet diese Entscheidungen über die innere Edge-Ebene an die Aktoren (rot, hier als Beispiel eine Ampel). Außerdem sendet jede Komponente der äußeren Edge-Ebene ihre Daten an die Cloud-Ebene, wo sie weiter verarbeitet werden und aktualisierte Modelle an die äußere Edge-Ebene zurückgesandt werden.

5.2.2 Relevante Gefährdungen

Angriffe können in einem, wie hier beschriebenen System auf allen Ebenen stattfinden:

- Endgeräte-Ebene
    - Auf der Endgeräte-Ebene können die Sensoren und Aktoren angegriffen werden. Beispielsweise könnten so die Sende-/Empfangseinheiten in vernetzten Fahrzeugen (C-ITS-Stationen) manipuliert oder Schlüsselmaterial für die Authentisierung extrahiert werden. Eine Besonderheit ist hier die spezielle Exponiertheit der Endgeräte im öffentlichen Raum. So sind Ampeln, Überwachungskameras, Sensoren am Straßenrand und ähnliches meist frei zugänglich und können somit vergleichsweise einfach direkt physisch angegriffen oder durch Unfälle beschädigt werden.
    - Ein Ausfall oder eine Kompromittierung einzelner Endgeräte kann zwar ein Risiko (z.B. Ampeln) darstellen, das lässt sich aber bei der Berechnung des gesamten Verkehrsflusses durch die Daten anderer Endgeräte ausgleichen.
    - Eine Manipulation der Daten auf dieser Ebene führt zu einem leicht verzerrten Gesamtbild, dies kann im Normalfall aber durch die anderen Sensoren ausgeglichen werden.

- Innere Edge-Ebene
    - Die innere Edge-Ebene ist bei diesem Szenario sehr exponiert, da die Komponenten am Straßenrand platziert werden und muss zusätzlich aufgrund ihrer zahlreichen (und manchmal mannigfaltigen) Verbindungen zu den Endgeräten speziell geschützt werden.
    - Ein Ausfall von einer oder mehreren Komponenten dieser Ebene kann die Gesamtlage durch "blinde Flecken" auf der Verkehrskarte ungenau und so zumindest teilweise unbrauchbar machen. Hier müsste zu einem großen Teil auf Erfahrungswerte zurückgegriffen werden, bis die Komponenten der inneren Edge-Ebene wieder ordnungsgemäß funktionieren.
    - Eine Manipulation der Daten auf dieser Ebene kann über lange Zeiträume zu einer Fehleinschätzung in den Vorhersagen und Modellen auf der äußeren Edge- und Cloud-Ebene führen. Hierdurch können die Vorteile der IoT-basierten Verkehrsregulierung mindestens teilweise zunichte gemacht werden.
- Äußere Edge-Ebene
    - Die äußere Edge-Ebene ist meist nur schwierig physisch erreichbar, da sie meist in Rechenzentren liegt. Sie ist aber mit einer Vielzahl an Komponenten der inneren Edge-Ebene verbunden.
    - Der Ausfall von Komponenten auf der äußeren Edge-Ebene würde zu einem Ausfall der smarten Verkehrsüberwachung und Optimierung führen.
    - Eine Manipulation der Daten auf dieser Ebene kann zu direkten Fehleinschätzungen und falschen bis gefährlichen Anweisungen an die Aktoren führen. Auch würden die Modelle in der Cloud auf Dauer unbrauchbar, sollte eine Manipulation über größere Zeiträume erfolgen.
- Cloud-Ebene
    - Die Cloud-Ebene liegt in einem Rechenzentrum und ist meist nicht so leicht physisch angreifbar. Sie ist mit der äußeren Edge-Ebene verbunden.
    - Sollten Dienste auf dieser Ebene oder die ganze Ebene ausfallen, so kann die äußere Edge-Ebene weiterhin voll funktionsfähig agieren, wird aber nicht mehr mit aktualisierten Daten und Modellen versorgt.
    - Eine Manipulation der Daten auf dieser Ebene würde die Modelle verfälschen, auf deren Basis in der äußeren Edge-Ebene Vorhersagen getätigt und Anweisungen an die Aktoren weitergegeben würden. Hierdurch würden die Vorteile einer IoT-basierten Verkehrsregulierung zunichte gemacht, oder sogar ins Gegenteil gekehrt.

Neben Angriffen auf einzelne Komponenten oder Ebenen, ist im Kontext des Edge Computings aber auch die Verbindung zwischen den einzelnen Komponenten und speziell den Ebenen zu beachten. So kann theoretisch ein Angriff auf der Endgeräte-Ebene als Einstiegspunkt genutzt werden, um auf die äußere Edge- oder Cloud-Ebene vorzudringen (Lateral Movement). Generell sollten Angriffsszenarien und Gefährdungen für die einzelnen Komponenten und die Verbindungen zwischen ihnen betrachtet werden.

Nachfolgend werden zwei Angriffsszenarien beispielhaft betrachtet:

5.2.3 Angriffsszenario 1: Angriff auf die Verfügbarkeit

5.2.3.1 Beschreibung

- Eine politisch motivierte Gruppe, die Überwachung prinzipiell ablehnt, will Kameras und andere Sensoren außer Betrieb setzen. Dafür geht sie auf verschiedene Arten gegen diese vor.

- Ein einfaches Mittel für die Gruppe ist Vandalismus und gezielte Zerstörung von wichtigen Elementen.
    - Durch rohe Gewalt werden Komponenten, die zur zentralen Verkehrsplanung eingesetzt werden und einfach zu erreichen am Straßenrand platziert sind, funktionsunfähig gemacht.
    - Außerdem gelangt die Gruppe durch Bestechung einer an der Planung beteiligten Person an die Pläne der Leitungsverläufe. Mit diesen Informationen kann die Kommunikation gezielt gestört werden (physische Leitungen durchtrennen, drahtlose Verbindungen durch Jamming stören), wodurch es zu einem längeren Ausfall des Kommunikationsnetzes, an welches mehrere Sensoren angeschlossen sind, kommt.
    - Zusätzlich werden durch das gezielte Kappen von Stromleitungen Steuerungseinheiten, die auf möglichst viele Sensoren und Aktoren Einfluss haben, außer Betrieb gesetzt.
- Durch Abhören der Kommunikationsleitungen erlangen Mitglieder der Gruppe Zugangsdaten für Komponenten der inneren Edge-Ebene.
    - Diese Zugangsdaten werden genutzt, um Zugriff auf mehrere Komponenten der inneren Edge-Ebene zu erlangen, wo sie Daten manipulieren oder löschen.
    - Infolge von DoS-Angriffen auf die äußere Edge-Ebene empfangen diese keine legitimen Daten mehr und es kommt zum Ausfall der Kommunikation mit der inneren Edge-Ebene und dadurch auch mit den Aktoren.

5.2.3.2 Handlungsempfehlungen

Um solche Angriffe zu erschweren, frühzeitig zu erkennen und die Auswirkungen gering zu halten, können folgende Maßnahmen umgesetzt werden:

- Endgeräte und Komponenten sollten schwer erreichbar angebracht und gesichert werden (bspw. durch Käfige, Schlösser, ...).
- Sensoren am Straßenrand sollten außerdem unauffällig angebracht werden.
- Kameras sollten auf potenzielle Angriffsziele ausgerichtet werden, um Angriffe frühzeitig zu erkennen.
- Zugriffe auf Geräte und Netz sollte auf registrierte Geräte begrenzt werden.
- Korruptionspräventionsmaßnahmen und -schulungen sollten für Mitarbeiter eingeführt werden.
- Die Kommunikation zwischen den einzelnen Ebenen und Komponenten sollte Ende-zu-Ende-verschlüsselt werden.
- Nachrichten/Verbindungen sollten bzgl. Authentizität und Integrität abgesichert werden (z.B. durch digitale Signaturen).
- Es sollte Multifaktor-Authentifikation genutzt werden.
- Mitigationsmaßnahmen für DoS-Angriffe sollten eingesetzt und nicht benötigte Protokolle (z.B. ICMP Pakete droppen, etc.) verboten werden.
- Für den Fall eines Ausfalls einer oder beider Edge-Ebenen, sollten die Aktoren (Ampeln, elektronische Verkehrsschilder, ...) auch autonom funktionieren und mit Standardeinstellungen versehen werden, um den geregelten Ablauf des Straßenverkehrs zu gewährleisten.
- Durch einen Abgleich mit einem zugrundeliegenden Verkehrsflussmodell kann der Ausfall einzelner Komponenten frühzeitig erkannt und eine schnelle Mitigation eingeleitet werden.
- Redundante Daten (bspw. Kameradaten zur Fahrzeugerkennung und Daten aus den Fahrzeugen selbst) sollten zur Anomalie-Erkennung abgeglichen werden.

5.2.3.3 Fazit / Netto-Risiken

Gerade in dem Gebiet der IoT für die Gesellschaft gibt es eine Vielzahl an Komponenten der inneren und äußeren Edge-Ebene, die teilweise im öffentlichen Raum physisch exponiert stehen. Diese sind ein einfaches Ziel für willkürlichen oder gezielten Vandalismus und sollten deshalb speziell vor physischen Angriffen geschützt werden. Hierbei müssen die Schutzmaßnahmen aber immer im Verhältnis zu der Relevanz für das Gesamtsystem stehen. Steuerungskomponenten, die an stärkeren Verkehrsknoten zum Einsatz kommen oder für die Planung des Verkehrsflusses der Stadt eingesetzt werden, müssen stärker geschützt werden als Steuerungskomponenten, die Ampelanlagen in Bereichen betreffen, die bei Ausfall gut kompensiert werden können.
Generell gelten hier für die einzelnen Komponenten ähnliche Gefährdungen und daraus abgeleitete Handlungsempfehlungen wie außerhalb des Edge Computing. Ein Hauptunterschied ist die weite Vernetzung der einzelnen Komponenten und Ebenen, durch die es viele Einstiegspunkte in das System und einen großen Spielraum für Bewegungen innerhalb des Systems (Lateral Movement) gibt.

5.2.4 Angriffsszenario 2: Angriff auf die Vertraulichkeit und Integrität

5.2.4.1 Beschreibung

- Eine Gruppe von Hackern wählt das Smart City System als lohnendes Ziel für ihre nächste Aktion aus. Ihr Plan ist es, einen Ransomeware Angriff gegen die Verkehrssteuerung durchzuführen, da dieses System essentiell für die Stadt ist.
- Durch Abhören der Kommunikationsleitungen erlangen Mitglieder der Gruppe Zugangsdaten einer Komponente der äußeren Edge-Ebene.
- Diese Zugangsdaten werden genutzt, um auf die Komponente der äußeren Edge-Ebene zuzugreifen.
- Von hier aus breiten sich die Angreifer durch Privilegien-Eskalation und Lateral Movement weiter im System aus.
- So erlangen sie Zugriff auf vertrauliche Daten, wie bspw. die Modelle und weitere Daten der Verkehrssteuerung.
- Zunächst erstellen die Angreifer eine Kopie der Daten auf ihren eigenen Systemen, denn diese lassen sich eventuell später für weitere Angriffe nutzen, oder verkaufen.
- Anschließend verschlüsseln sie die Daten auf den Komponenten der äußeren Edge-Ebene und stellen eine Lösegeldforderung für den kryptografischen Schlüssel an die Stadtverwaltung.
- Solange die Daten nicht wiederhergestellt werden können, ist die Verkehrssteuerung lahm gelegt.

5.2.4.2 Handlungsempfehlungen

Um solche Angriffe zu erschweren, frühzeitig zu erkennen und die Auswirkungen gering zu halten, können folgende Maßnahmen umgesetzt werden:

- Leitungen sollten Ende-zu-Ende verschlüsselt werden.
- Nur Geräte, die entsprechend unterschiedliches Schlüsselmaterial (Private Keys) einsetzen, sollten verwendet werden.
- Die Standardkonfiguration von Geräten sollte angepasst und das Benutzen von Standardpasswörtern vermieden werden.
- Es sollte Multifaktor-Authentifikation genutzt werden.
- Defense in Depth Prinzipien sollten umgesetzt werden (z. B. Secrets-Management in den Netzen der äußeren Edge-Ebene).

- Es sollte eine umfangreiche Backup-Strategie vorhanden sein und umgesetzt werden (speziell auf der äußeren Edge- und Cloud-Ebene).
- Durch einen Abgleich mit einem zugrundeliegenden Verkehrsflussmodell kann die Veränderung einzelner Komponenten frühzeitig erkannt und eine schnelle Mitigation eingeleitet werden.
- Redundante Daten (bspw. Kameradaten zur Fahrzeugerkennung und Daten aus den Fahrzeugen selbst) sollten zur Anomalie-Erkennung abgeglichen werden.

5.2.4.3 Fazit / Netto-Risiken

Generell gelten hier für die einzelnen Komponenten ähnliche Gefährdungen und daraus abgeleitete Handlungsempfehlungen wie außerhalb des Edge Computing. Ein Hauptunterschied ist die weite Vernetzung der einzelnen Komponenten und Ebenen, durch die es viele Einstiegspunkte in das System und einen großen Spielraum für Bewegungen innerhalb des Systems (Lateral Movement) gibt.

Geeignete Backup-Maßnahmen sowie der Aufbau von Redundanzen bei den Edge-Komponenten sollten hier bedacht werden. Somit verringert man seine eigene Erpressbarkeit und kann die Systeme bei einem Angriff, oder einem technischen Defekt, möglichst schnell wieder nutzen. Auch sollte bei einem Wechsel auf Edge-Komponenten abgewogen werden, in wie weit man herkömmliche Systeme abschafft oder zurück baut. Gerade in einem so kritischen Gebiet wie dem Straßenverkehr, sollten die "klassischen" Mittel der Verkehrssteuerung erhalten bleiben, da so bei einem Ausfall der Smart City Systeme wieder in den herkömmlichen Modus gewechselt werden kann.

5.3 Use Case 2: IoT für Industrie (Predictive Maintenance)

5.3.1 Definition

Der Begriff "Predictive Maintenance", nachfolgend PM, bedeutet übersetzt "vorausschauende Instandhaltung" und bezeichnet somit die proaktive Wartung von Maschinen auf Basis zuvor erhobener Mess- und Produktionsdaten. Durch unerwartete Maschinenausfälle ausgelöste Produktionsverzögerungen, wie sie bei der Anwendung reaktiver Instandhaltung auftreten können, sollen dadurch ebenso minimiert werden wie durch überflüssige Wartungsarbeiten ausgelöste Kosten, wie sie bei der Anwendung präventiver Instandhaltung auftreten können. Das Vorgehen hierzu baut grundsätzlich auf drei Schritten auf: Erhebung von Sensordaten, Verarbeitung von Sensordaten und Berechnung einer Prognose.

Die Erhebung der Sensordaten erfolgt kontinuierlich und verwendet IoT-Sensoren, welche die Maschine selbst, deren Peripherie und deren Umgebung erfassen. Beispiele für üblicherweise erhobene Messdaten sind die Beschleunigung von Fahrzeugachsen zur Kontrolle derer Belastung, die Vibrationen an einer Welle zur Kontrolle derer Abnutzung oder auch die Erhebung der Temperatur von Motoren zur Kontrolle derer Kühlung. Um basierend auf jener Grundlage eine Prognose aufstellen zu können, werden die Daten automatisiert anhand eines Modells analysiert und auf unerwartete Abweichungen von diesem untersucht. Das Modell kann hierbei auf Expertenwissen und mathematischen Modellierungen oder Machine Learning-Verfahren aufbauen. Als Initialbestand des Modells können zuvor gesammelte Datenbestände der eigenen Maschinen oder externe Datensätze verwendet werden. Später können neu erhobene Daten regelmäßig in das bestehende Modell eingearbeitet werden. Das Ergebnis der Analyse und deren Auswertung sind eine Einschätzung der Restnutzungsdauer der einzelnen Komponenten der Maschine, deren Daten erhoben wurden. Basierend auf dieser Einschätzung können dann gezielt Wartungsarbeiten vorgenommen werden.

Zur Umsetzung von PM werden oft reine Cloud-Dienste in Anspruch genommen, doch auch Edge Computing-Lösungen gewinnen in diesem Bereich an Bedeutung. Die äußere Edge-Ebene kann beispielsweise dazu dienen, Maschinen eines Maschinenbauers in einzelnen Regionen oder unterschiedliche Standorte eines Betreibers zusammenzufassen. In Anlehnung an die vorhandene Literatur zum Thema Predictive Maintenance beschränkt sich dieser Use Case jedoch auf die innere Edge- und die Cloud-Ebene. Für die Aufteilung der einzelnen Predictive Maintenance-Schritte auf die innere Edge- und die Cloud-Ebene gibt es weiterhin unterschiedliche Schemata. Die Erstellung des initialen Predictive Maintenance-Modells

geschieht meist auf der Cloud-Ebene. Dieses Modell wird dann in die innere Edge-Ebene integriert, wo die Sensordaten der Endgeräte anhand dessen aggregiert und vorausgewertet werden. Eine solche Vorauswertung umfasst zumindest das Filtern und Aufbereiten der erhobenen Daten zur besseren Weiterverwendung. Je nach Schema kann nun die Berechnung einer Prognose für die Restnutzungsdauer der Maschinen bereits auf der inneren Edge-Ebene stattfinden, oder auf die Cloud-Ebene verlagert werden. In letzterem Fall werden die vorausgewerteten Daten an die Cloud übermittelt und dort optional einem zusätzlichen, rechenintensiveren Auswertungsmechanismus zugeführt. Auch die Einbindung der neuerfassten Daten in das Predictive Maintenance-Modell kann entweder auf der Cloud- oder der inneren Edge-Ebene durchgeführt werden.

Nachfolgend wird das Szenario eines großen nationalen Unternehmens, welches in der Fertigungs-Industrie tätig ist und seine Produkte für durchschnittlich 12.000€ pro Stück verkauft, betrachtet. Einen integralen Bestandteil des Produktionszyklus dieses Unternehmens stellen dabei dessen Fertigungsroboter dar. Da Produktionsstillstände in Folge unerwarteter Ausfälle der Fertigungsroboter für das Unternehmen mit Kosten von 10.000€ pro Minute behaftet sind, bezieht es einen Edge-basierten Predictive Maintenance-Dienst. Zu diesem Zwecke wurden alle Fertigungsroboter mit jeweils vier Sensoren ausgestattet: einer Wärmebildkamera zur Erhebung der Temperatur, einem Hygrometer zur Erhebung der Luftfeuchtigkeit, einem Druckmesser zur Erhebung des Luftdrucks und einem Schwingungsmessgerät zur Durchführung von Schwingungsanalysen. Das Predictive Maintenance-Modell berücksichtigt die Daten der vier Sensoren im Kontext der Nutzungsdauer, -art, sowie -intensität ihres zugehörigen Fertigungsroboters und wurde initial durch die Machine Learning-Algorithmen des PM-Anbieters berechnet. Die Trainingsdaten wurden in Form von Historiendaten von dem Unternehmen zur Verfügung gestellt.

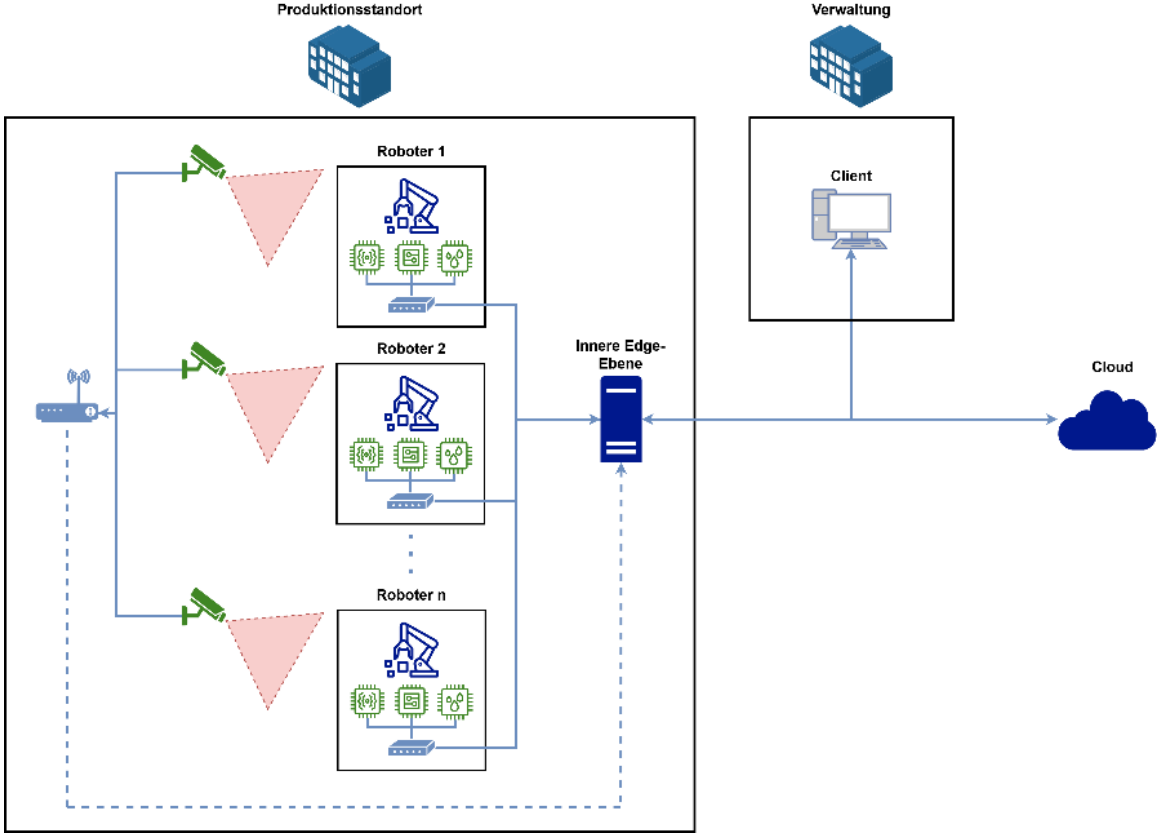

Abb. 6 Umsetzung von Predictive Maintenance

Diese Grafik (Abb.6) gibt eine grobe Übersicht über einen exemplarischen Aufbau der IoT-basierten Umsetzung von Predictive Maintenance und den darin verwendeten Komponenten der inneren Edge-Ebene und Cloud-Diensten. Die Daten der Sensoren (grün) werden gesammelt und an die innere Edge-Ebene weitergeleitet. Die verarbeiteten Daten werden zur Cloud geschickt und in regelmäßigen Abständen werden aktualisierte Modelle aus der Cloud in die innere Edge-Ebene gespiegelt. Die Verwaltung des Unternehmens kann über einen Client auf die innere Edge- und die Cloud-Ebene zugreifen und somit auf

die berechneten Restnutzungszeiten reagieren, zum Beispiel indem sie Ersatzteile bestellt oder Wartungsarbeiten initiiert.

5.3.2 Relevante Gefährdungen

Angriffe können in einem, wie hier beschriebenen, System auf allen Ebenen stattfinden:

- Endgeräte-Ebene
    - Auf der Endgeräte-Ebene können die Sensoren und Aktoren angegriffen werden. Zu beachten ist hier die teilweise Exponiertheit der Endgeräte, welche in einem Fabrikgebäude stehen. Dabei sind Kameras, die frei im Raum platziert sind, prinzipiell einfacher physisch anzugreifen als bspw. Sensoren, die in Maschinen verbaut sind.
    - Ein Ausfall oder eine Kompromittierung einzelner Endgeräte kann zu Ungenauigkeiten der Daten und damit Fehlern in der Qualität des PM-Prozesses führen.
    - Endgeräte können so manipuliert werden, dass sie keine, fehlerhafte oder falsche Daten übertragen. Fehlerhafte Daten können dabei beispielsweise Daten sein, die falsch kodiert sind und in Folge nicht ausgewertet werden können. Falsche Daten hingegen können Daten sein, die gezielt verändert wurden.
- Innere Edge-Ebene
    - Die innere Edge-Ebene ist meist nicht direkt physisch zugänglich, muss aber aufgrund ihrer zahlreichen (und manchmal mannigfaltigen) Verbindungen zu den Endgeräten speziell geschützt werden.
    - Ein Ausfall der Komponente dieser Ebene führt dazu, dass keine lokale Auswertung der Sensordaten mehr möglich ist. Die übersandten Sensordaten werden nicht mehr gesammelt, gehen möglicherweise verloren und werden nicht mehr an die Cloud-Ebene weitergeleitet. Es kann bei (längeren) Ausfällen zu einer Beeinträchtigung oder einem Ausfall der gesamten PM an diesem Standort kommen.
    - Eine Manipulation der Daten auf dieser Ebene kann zu einer falschen lokalen Auswertung und damit Fehlern in den Vorhersagen des PM führen. Es werden falsche Daten an die Cloud weitergeleitet und gerade über längere Zeiträume können die Modelle in der Cloud verfälscht und unbrauchbar gemacht werden. Die lokale Auswertung auf der inneren Edge-Ebene anhand der verfälschten Modelle kann wiederum zu falschen Wartungsentscheidungen führen.
- Cloud-Ebene
    - Die Cloud-Ebene liegt meist in Rechenzentren und ist dadurch nur schwierig physisch angreifbar. Sie ist mit der inneren Edge-Ebene verbunden.
    - Sollte sie ausfallen, so kann die innere Edge-Ebene weiterhin voll funktionsfähig agieren, wird aber nicht mehr mit aktualisierten Modellen versorgt - aufgrund dessen können die lokalen Auswertungen unnötige Wartungsvorgänge oder nicht vorhersehbare Ausfälle zur Folge haben.
    - Eine Manipulation der Daten auf dieser Ebene würde die Modelle verfälschen, auf deren Basis in der inneren Edge-Ebene Vorhersagen getätigt werden - aufgrund dessen können die lokalen Auswertungen unnötige Wartungsvorgänge oder nicht vorhersehbare Ausfälle zur Folge haben. Gerade bei KI-Modellen ist allerdings nicht mit allzu großen Änderungen der Modelle in wenigen Schritten zu rechnen.
    - Eine Kompromittierung der Cloud-Ebene kann zu unberechtigten Zugriffen auf die Daten führen. Aus den Daten können möglicherweise geschäftskritische Informationen (wie beispielsweise Auslastung der Maschinen und damit zur Auftragslage) abgeleitet werden.

Neben Angriffen auf einzelne Komponenten oder Ebenen, ist im Kontext des Edge Computings aber auch die Verbindung zwischen den einzelnen Komponenten und speziell den Ebenen zu beachten. So kann theoretisch ein Angriff auf der Endgeräte-Ebene als Einstiegspunkt genutzt werden, um auf die innere Edge- oder Cloud-Ebene vorzudringen (Lateral Movement). Generell sollten Angriffsszenarien und Gefährdungen für die einzelnen Komponenten und die Verbindungen zwischen ihnen betrachtet werden.

Nachfolgend werden zwei Angriffsszenarien beispielhaft betrachtet:

5.3.3 Angriffsszenario 1: Angriff durch einen Außentäter

5.3.3.1 Beschreibung

- Ein Konkurrent des Unternehmens möchte diesem unauffällig schaden, um seine eigene Stellung im Markt zu stärken und ohne selbst in Bedrängnis zu geraten. Da die Endgeräte- und die innere Edge-Ebene oft verletzlicher als die Cloud-Ebene gegenüber IT-Angriffen sind, werden diese zu einem der Angriffsziele.
- Der Konkurrent verschafft sich externen Zugriff auf die Steuerung des Verwaltungs-Clients, beispielsweise durch die Durchführung eines Spear-Phishing-Angriffes. Über den Verwaltungs-Client hat der Konkurrent dann Zugriff auf die Steuerung der Fertigungsroboter und der inneren Edge-Ebene.
- Der Konkurrent beobachtet die von den eingenommenen Endgeräten gemessenen Sensordaten und ermittelt über diese ein Intervall von Idealdaten, welche bei Vorliegen eines robusten Gesundheitszustandes der Fertigungsroboter gemessen werden sollten.
- Den Zugriff auf die Steuerung der Fertigungsroboter verwendet der Konkurrent, um Änderungen an deren Konfiguration durchzuführen, die den Verschleiß der Roboter im Vergleich zu den ursprünglichen Konfigurationen schneller vorantreiben.
- Um seinen Eingriff zu verschleiern, manipuliert der Konkurrent Anwendungen der inneren Edge-Ebene so, dass die eigentlich gemessenen Sensordaten verworfen und durch Werte aus dem zuvor ermittelten Idealintervall in die PM-Lösung des Unternehmens eingespeist werden.
- Die PM-Lösung analysiert die gefälschten Daten und überschätzt basierend auf diesen die Restnutzungsdauer der Fertigungsroboter: Der echte nutzungsbedingte Verschleiß der Fertigungsroboter bleibt bis zu deren unerwartetem Ausfall unerkannt.
    - Es erfolgt ein Stillstand der Produktion bis zur Reparatur oder dem Austausch der ausgefallenen Roboter, bzw. Roboterkomponenten (finanzieller Verlust in Höhe von 10.000€ pro Minute).
    - Falls der Ausfall während der aktiven Produktion stattfand, drohen zusätzlich potentiell
        - die Beschädigung des aktuell gefertigten Produkts (finanzieller Verlust je nach Schaden in Höhe von bis zu 12.000€ Euro).
        - eine Verletzung des Angestellten, welcher den ausgefallenen Fertigungsroboter bedient oder dessen Arbeit ergänzt hat.
    - Da die Manipulation der Roboter verschleiert wird, können durch deren inkorrekte Konfiguration bereits vor dem Ausfall Mängel an den gefertigten Produkten entstehen, die zu einem finanziellen oder Image-Schaden des Unternehmens führen können.
- In Folge des unerwarteten Ausfalls soll das auf der Cloud antrainierte PM-Modell aktualisiert werden, zu welchem Zwecke die manipulierten Sensordaten an die Cloud übermittelt und in den Machine Learning (ML)-Trainingsprozess eingebunden werden. Basierend auf dem verfälschten Modell können die Sensorwerte eines Roboters in einem robusten Gesundheitszustand als Anzeichen auf einen weiteren Ausfall gedeutet und die Restnutzungsdauer unterschätzt werden.
    - Beauftragung der Wartung gesunder Roboter, dadurch vermeidbare Kosten.

- Rücksetzung des PM-Modells auf einen Stand vor Einschleusung der manipulierten Daten ist notwendig, dadurch gehen potentiell auch echte Daten verloren.

5.3.3.2 Handlungsempfehlungen

Um solche Angriffe zu erschweren, frühzeitig zu erkennen und die Auswirkungen gering zu halten, können folgende Maßnahmen umgesetzt werden:

- Es sollte ein standardisiertes Konfigurationsmanagement eingesetzt werden.
- Verantwortliche sollten sensibilisiert und regelmäßige Schulungen (beispielsweise bzgl. Authentisierungsmechanismen) durchgeführt werden.
- Für die Kommunikation zwischen den einzelnen Ebenen sollten Ende-zu-Ende-verschlüsselte Leitungen eingesetzt werden und auf registrierte Geräte beschränkt werden.
- Es sollte Multifaktor-Authentifikation genutzt werden.
- Für relevante Daten, wie die Sensordaten und das PM-Modell, sollte eine Datensicherung durchgeführt werden.
- Die in die einzelnen Komponenten und Dienste eingehenden sowie aus den einzelnen Komponenten und Dienste ausgehenden Daten sollten protokolliert werden. Die Protokolle sollten regelmäßig, potenziell anhand eines Plausibilitätsmodells, ausgewertet werden.
- Die IoT-Sensoren könnten ihre Sensordaten signiert übermitteln. Falls möglich sollen hier nur Sensordaten von registrierten Sensoren zugelassen werden. Die Signaturen könnten von der PM-Lösung überprüft werden.
- Für das Predictive Maintenance-Modell sollte eine Black Box-Variante verwendet werden, welche nach einer ersten erfolgreichen Trainingsphase nicht weiter trainiert wird.
- Das Predictive Maintenance-Modell sollte in Hinsicht auf dessen Robustheit und Resilienz analysiert werden, um einen möglichst großen Aufwand bei der Sensormanipulation vorauszusetzen.
- Die bezogene Predictive Maintenance-Lösung sollte selbst Maßnahmen zur Prävention und Detektion manipulierter Eingabedaten, zum Beispiel das Ausbleiben erwartbarer Ausreißer, ermöglichen.

5.3.3.3 Fazit / Netto-Risiken

Einer der wichtigsten Aspekte zur Absicherung Edge-basierter Predictive Maintenance-Anwendungen vor dem dargestellten Angriffspfad ist die allgemeine Absicherung der Komponenten der inneren Edge-Ebene vor unerwünschtem Eindringen und Einspielen von Nachrichten. Derartige Angriffe können durch das Umsetzen der Handlungsempfehlungen zwar nicht ausgeschlossen, jedoch signifikant erschwert werden. Durch die Verwendung verschlüsselter Leitungen bleiben dem Angreifer Daten, die dessen Vorgehen erleichtern würden, vorenthalten; die Verwendung von Multi-Faktor-Authentisierung und Signaturen erschwert es dem Angreifer, unbemerkt in das System einzudringen und dieses zu beeinflussen; durch eine kontinuierliche Protokollierung und deren Auswertung wird es möglich, die Anwesenheit eines Angreifers zu erkennen, noch bevor dieser den gewünschten Schaden ausrichten konnte.

Da die Absicherung der Machine Learning-Algorithmen und des Predictive Maintenance-Modells dem Anbieter des Predictive Maintenance-Dienstes unterliegt, fokussiert sich der Handlungsbedarf des Unternehmens in dieser Hinsicht auf die Auswahl eines den eigenen Sicherheitsanforderungen entsprechenden Anbieters. Insbesondere die Wahl eines Predictive Maintenance-Dienstes, der einem Black Box-Modell folgt, kann die Gefahr von Data Poisoning nach dem erfolgreichen Abschluss der Trainingsphase vollständig ausschließen. Das Restrisiko einer Evasion Attack kann nicht pauschal bestimmt

werden, wird aber durch die Kombination aus Anbieter-seitigen Sicherheitsmaßnahmen und den Anwender-seitigen Maßnahmen zur Vermeidung manipulierter Eingabedaten reduziert.

5.3.4 Angriffsszenario 2: Angriff durch einen Innentäter

5.3.4.1 Beschreibung

- Ein Mitarbeiter des Fertigungsunternehmens, dem seiner Meinung nach zu Unrecht gekündigt wurde, möchte sich an seinem letzten Tag bei der Firma rächen.
- Obwohl der Mitarbeiter nicht mit der Überwachung der PM-Lösung betraut wurde, hat er Zugriff auf den Client, über welchen die Komponente der inneren Edge-Ebene erreicht werden kann. Er nutzt für seinen Angriff einen Test-Account mit Administratorrechten, der in der Testphase der PM-Lösung erstellt und nie gelöscht wurde.
- Von hier aus löscht er die auf der Cloud-Ebene hinterlegten Modelle und weiteren Dateien der PM-Lösung.
- Durch die gelöschten Daten wird der Cloud-Anteil des PM ausfallen, bis der Vorfall bemerkt und die Daten wiederhergestellt sind oder ein neues Modell erstellt wurde.
- Er findet die Schnittstelle, die wichtige Ereignisse an die zuständigen Abteilungen sendet und schickt Warnungen für den Ausfall mehrerer, besonders teurer Bauteile ab.
- Hierdurch werden am nächsten Tag Bestellungen für die entsprechenden Ersatzteile erstellt.

5.3.4.2 Handlungsempfehlungen

Um solche Angriffe zu erschweren, frühzeitig zu erkennen und die Auswirkungen gering zu halten, können folgende Maßnahmen umgesetzt werden:

- Rechte und Rollen sollten geeignet auf eine festgelegte Rollendefinition vergeben werden (Least Privilege Prinzip). Insbesondere sollten Identitäten, die nicht mehr benötigt werden (z.B. Test-Accounts nach Beendigung der Test-Phase), entfernt und die Produktionsumgebung insbesondere bezüglich der Rechtevergabe gehärtet werden. Es sollte kein generalisierter Administratorzugriff vorliegen, damit eine Nachvollziehbarkeit der Aktivitäten erfolgen kann.
- Es sollte Multifaktor-Authentifikation genutzt werden.
- Nutzer mit mehreren Rollen sollten für diese separate Accounts bekommen (separation of duties).
- Änderungen an bspw. Konfigurationen sollten geloggt werden. Kritische Änderungen sollten einen Alarm auslösen.
- Für relevante Daten sollten Backups erstellt werden.

5.3.4.3 Fazit / Netto-Risiken

Ein geeignetes Rechte- und Rollen-System, in dem jede Identität nur die für die Erfüllung ihrer Tätigkeit notwendigen Rechte erhält und nach Erfüllung der Tätigkeit rechtzeitig entzogen bekommt, ist essentiell, um Innentätern, oder von Angreifern übernommenen Accounts, möglichst wenig Spielraum zu lassen. Auch sollten möglichst alle Änderungen am System, bzw. alle Aktionen und wer diese wann vorgenommen hat, geloggt werden. Somit können Fehler oder Angriffe anschließend nachvollzogen, teilweise rückgängig gemacht und potentiell zukünftig verhindert werden. Ein Innentäter kann zwar nie ganz verhindert werden, seine Möglichkeiten sollten aber so weit wie möglich eingeschränkt werden.

Geeignete Backup-Maßnahmen, bis hin zu der Nutzung einer Multi Cloud-Strategie, sollten bedacht werden. Somit verringert man seine eigene Erpressbarkeit und kann die Systeme bei einem Angriff, oder einem technischen Defekt, möglichst schnell wieder nutzen.

5.4 Use Case 3: Datenverarbeitung und Enterprise Security (Hochfrequenzhandel an der Börse)

5.4.1 Definition

Nachfolgend soll ein Use Case beschrieben werden, in dem Ultra Low Latency (ULL)-Anwendungen zum Einsatz kommen, für welche beispielsweise ITaaS-Edge-Komponenten gut geeignet sind. Als leicht verständliches Beispiel wird Hochfrequenzhandel an der Börse gewählt, wo Angriffe umfassende Auswirkungen haben könnten.

Käufe und Verkäufe von Wertpapieren laufen hierbei automatisiert ab. Handelsteilnehmer versuchen bei dieser Art des Handels Möglichkeiten zu nutzen, die Geschwindigkeitsvorteile beim Abschluss eines Handels einbringen. Damit die Zeit zwischen Absenden und Empfang einer Order möglichst kurz ist, wird in dem beschriebenen Anwendungsfall eine oder mehrere ITaaS-Edge-Komponente/n im Rechenzentrum eines Handelsplatzes an der Börse, also auf der inneren Edge-Ebene, platziert. Diese Edge-Komponenten kommunizieren über eine verschlüsselte Verbindung mit einem Rechenzentrum eines Cloud-Anbieters, über dessen Cloud die Verwaltung der Systeme auf der Edge-Komponenten organisiert und zeitunkritische Aufgaben durchgeführt werden. Die Edge-Komponenten sind über lokale Gateways über eigens für ULL ausgelegte Netz-Interfaces, so genannte ULL-NICs, mit dem Netz des Handelsplatzes verbunden. Wegen der hohen Latenz-Kritikalität werden die Edge-Komponenten über ein 1PPS-Zeitsignal mit der Infrastruktur des Handelsplatzes synchronisiert. Die Anwendung auf den Edge-Komponenten werden so in die Lage versetzt, auf Kursänderungen extrem schnell zu reagieren und Handelsaufträge abzusetzen. Für die Käufe und Verkäufe sind verschiedene Teilnehmer an den Handelsplatz mit eigenen Verarbeitungskomponenten angeschlossen. Da es bei diesem Szenario um sehr geringe Latenzen geht, werden keine Komponenten auf der äußeren Edge-Ebene benötigt. Diese Art des Handels ist in Deutschland strengen Regularien unterlegen, da bei Fehlern starke Kursschwankungen entstehen könnten.

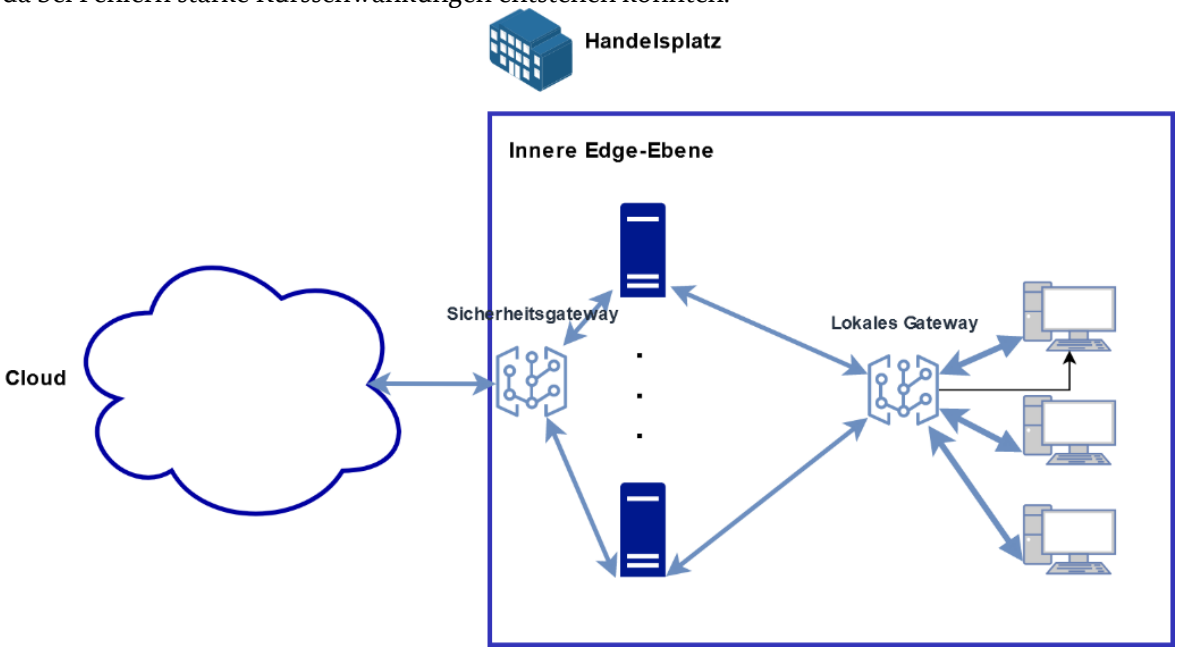

Abb. 7 Beispiel für den Einsatz von Edge-Komponenten beim Hochfrequenzhandel an der Börse

In Abb. 7 wird beispielhaft dargestellt, wie der Einsatz einer oder mehrerer Edge-Komponenten beim Hochfrequenzhandel an der Börse aussehen könnte. Im Bild sind beispielhaft mehrere ITaaS-Edge-Komponente am Handelsplatz der Börse, also auf der inneren Edge-Ebene, untergebracht. Über das Netz des Handelsplatzes wird auf die Komponenten zugegriffen. Hierüber greifen die verschiedenen Teilnehmer, die am Hochfrequenzhandel teilnehmen, automatisiert auf die Komponenten zu. Die Edge-Komponenten kommunizieren über eine verschlüsselte Verbindung mit einem Rechenzentrum eines Cloud-Anbieters, über dessen Cloud die Verwaltung der Systeme auf den Edge-Komponenten organisiert und zeitunkritische Aufgaben durchgeführt werden. Eine äußere Edge-Ebene gibt es in diesem Szenario nicht.

In den folgenden Abschnitten werden Gefährdungen für das oben beschriebene Szenario betrachtet, sowie Handlungsempfehlungen aufgezeigt.

5.4.2 Relevante Gefährdungen

Angriffe können in einem, wie hier beschriebenen System auf folgenden Ebenen stattfinden:

- Endgeräte-Ebene
    - Auf der Endgeräte-Ebene können die IT-Systeme angegriffen werden. Da sich die meisten IT-Systeme in geschlossenen Gebäuden mit Gebäudesicherungsmaßnahmen befinden werden, sind physische Angriffe eher unwahrscheinlich, jedoch nicht unmöglich. Prinzipiell könnten auch Endgeräte, die nicht gut geschützt sind, angeschlossen werden. Diese könnten Ziel von Angreifern werden, die versuchen über das Endgerät Schadsoftware zu vertreiben oder Manipulationen vorzunehmen.
    - Ein Ausfall einzelner Endgeräte kann zu fehlenden Handelsaktionen führen, die aber nur zu Nachteilen für den Betreiber des Endgerätes und seiner Kunden führt und damit hier nicht betrachtet wird.
    - Endgeräte können so manipuliert werden, dass sie keine, fehlerhafte oder falsche Daten übertragen. Fehlerhafte Daten können dabei beispielsweise Daten sein, die falsch kodiert sind und in Folge nicht ausgewertet werden können. Sollten diese in hohem Maß auftreten, kann es zu Verzögerungen auf anderen Ebenen führen, die die ULL des Gesamtszenarios beeinträchtigen und den Handelsverkehr beeinflussen.
- Innere Edge-Ebene
    - Die innere Edge-Ebene ist physisch nicht exponiert, muss aber aufgrund ihrer möglicherweise zahlreichen Verbindungen zu den Endgeräten speziell geschützt werden.
    - Die Edge-Komponenten bieten die Möglichkeit, dass auf ihnen viele Anwendungen/Dienste ähnlich wie in der Cloud parallel laufen. Bei unzureichender Isolation können unberechtigte Zugriffe auf Daten oder Anwendungen erfolgen.
    - Ein Ausfall von einer oder mehreren Edge-Komponenten kann dazu führen, dass Daten von Kunden verloren gehen und diese Verluste erfahren.
    - Eine Manipulation der Daten auf dieser Ebene kann zu falschen Gewinnausschüttungen führen. Im schlimmsten Fall könnte es zu einer Kettenreaktion kommen, die den Markt verändert.
- Cloud-Ebene
    - Die Cloud-Ebene liegt in einem Rechenzentrum beim Anbieter und ist dadurch nur schwierig physisch angreifbar.
    - Sollte die Cloud-Ebene ausfallen, können keine Konfigurationen an die Edge-Ebene weitergeleitet werden, ältere bleiben jedoch auf der Edge-Ebene erhalten. Möglicherweise kann die Edge-Ebene nicht mehr bedient werden.
    - Ressourcen der Cloud-Ebene können direkt mit der Edge-Ebene verbunden werden, so dass bei entsprechender Berechtigung Schadprogramme aus der Cloud auf die Edge-Ebene übertragen werden könnten.
    - Eine Manipulation der Daten auf dieser Ebene könnte die Daten auf allen Ebenen kompromittieren.

Neben Angriffen auf einzelne Komponenten oder Ebenen, ist im Kontext des Edge Computing aber auch die Verbindung zwischen den einzelnen Komponenten und speziell den Ebenen zu beachten. So kann theoretisch ein Angriff auf der Endgeräte-Ebene als Einstiegspunkt genutzt werden, um auf die innere Edge-

oder Cloud-Ebene vorzudringen (Lateral Movement). Generell sollten Angriffsszenarien und Gefährdungen für die einzelnen Komponenten und die Verbindungen zwischen ihnen betrachtet werden.

Im folgenden Abschnitt werden zwei Szenarien beispielhaft betrachtet.

5.4.3 Angriffsszenario 1: Angriff durch Außentäter über die Edge-Ebene

5.4.3.1 Beschreibung

- Es greifen verschiedene Teilnehmer automatisiert mit ihren Verarbeitungskomponenten auf die Edge-Komponenten des Handelsplatzes der Börse zu, um Handel zu betreiben.
- Ein angeschlossener Teilnehmer, der Administrationsrechte auf eine der Komponenten hat, um Ressourcen für den schnelleren Handel dynamisch konfigurieren zu können, wird Ziel eines Cyber-Angriffs.
- Der Angreifer erhält Zugriff auf die Verarbeitungskomponente dieses Teilnehmers. Durch Privilegien-Eskalation und Lateral Movement arbeitet er sich, wo es möglich ist, durch die angeschlossenen Systeme der Edge-Komponenten.
- Der Angreifer verteilt Schadsoftware oder Hintertüren über die Verarbeitungskomponente auf die Syteme der Edge-Komponente. Von hier versucht sich die Schadsoftware, weiter zu verbreiten.

Er könnte hierzu folgendermaßen vorgehen:

- Der Angreifer analysiert den Verkehr zu der Handelsplattform.
- Er identifiziert über Abfragen die auf der Handelsplattform eingesetzten Systeme.
- Er könnte dabei festgestellen, dass auf einem System der Edge-Komponente eine veraltete Software eingesetzt wird.
- Über diese Schwachstelle könnte eine Ransomware eingespielt werden, die die Daten auf dem vulnerablen System verschlüsselt und versucht sich auf weitere Systeme der Edge-Komponente zu verbreiten.
- Alternativ könnte er versuchen, die Struktur der Transaktionen kennenzulernen und je nach Rechten, die er erbeutet hat, versuchen, Transaktionen zu löschen, zu verändern oder weitere hinzuzufügen.

5.4.3.2 Handlungsempfehlungen

Um solche Angriffe zu erschweren, frühzeitig zu erkennen und die Auswirkungen gering zu halten, können folgende Maßnahmen umgesetzt werden:

- Es sollte eine engmaschige und kurz getaktete Überwachung der Systeme etabliert werden, um Anomalien sehr schnell zu erkennen.
- Es sollte ein Plausibilitätsprüfung stattfinden, um Differenzen schnell erkennen zu können und notwendige Mitigationsmaßnahmen einleiten zu können.
- Zugriffsrechte sollten auf das nötigste Mindestmaß (Zero Trust / Assume Breach-Ansatz) eingeschränkt sein, um zu verhindern, dass unnötige Zugriffe stattfinden können (beispielsweise Informationen über Systeme der Handelsplattform nach außen gegeben werden).
- Administratoren sollten eine intensive Schulung bekommen, da insbesondere das Berechtigungsmanagement sehr komplex und damit auch schwieriger zu bedienen sein kann. Die Rechtevergabe und Gruppenrichtlinien sollten sehr restriktiv vergeben werden.
- Handelsteilnehmer sollten bezogen auf solche Angriffe geschult werden.

- Ein Konzept zum Schutz vor Schadprogrammen sollte erstellt und Maßnahmen zur Isolation befallener Komponenten sollten bereitgestellt werden.
- Regelmäßige Updates von Softwarekomponenten sollten durchgeführt und hierfür die Administratoren sensibilisiert und verpflichtet werden.

5.4.3.3 Fazit / Netto-Risiken

Es wird ein Risiko darin gesehen, dass Komponenten automatisiert auf die Edge-Komponente/-n zugreifen, die nicht unter dem Einfluss des Betreibers der Hochfrequenzhandelskomponente selbst liegen. Hierbei besteht grundsätzlich das Risiko, dass diese mit Schadsoftware behaftet sind oder Zugriff durch unberechtigte Personen initiiert werden kann. Das Risiko kann verringert werden, indem die Zugriffsmöglichkeiten auf ein Minimum begrenzt werden und nur die nötigen Transferinformationen in einem Format übergeben werden, über welches keinerlei Schadsoftware transportiert werden kann.

5.4.4 Angriffsszenario 2: Angriff durch Innentäter über die Edge-Ebene

5.4.4.1 Beschreibung

- Da die Edge-Komponenten mandantenfähig sind, wird auf einer Komponente neben der Anwendung für den Hochfrequenzhandel eine Verwaltungssoftware für die Mitarbeiter des Handelsplatzes untergebracht. Die Verantwortlichen entscheiden dies zu tun, da der Zugriff über physisch getrennte Netzverbindungen erfolgt und die Verwaltungssoftware nur geringe Rechenkapazitäten benötigt. Es wird angenommen, dass daher die Latenz der Handelsplattform durch den normalen Betrieb beider Anwendungen auf derselben Plattform nicht beeinträchtigt wird.
- Ein Mitarbeiter oder Servicemitarbeiter einer Drittfirma, der Zugriff auf die Verwaltungssoftware hat, versucht durch Sabotage die Anwendung für die Hochfrequenzhandelsplattform zu stören.
- Die dadurch unter Umständen schwankenden Kurse nutzt der Angreifer für sich gewinnbringend aus oder er schädigt Handelsplatzteilnehmer, indem er durch viele Transaktionen hohe Kosten für die Handelsteilnehmer verursacht.
- Da er durch seine Tätigkeit bei der Verwaltungsplattform Kenntnis über die Protokollierungsmaßnahmen der Komponente besitzt, versucht er seine Tätigkeiten zu verschleiern.

Er könnte dafür folgende Wege gehen:

- Er stört die Edge-Komponente durch eine Ressourcen-intensive Aufgabe.
- Er erhält physischen Zugang zur Edge-Komponente und verändert Netzkonfigurationen, inszeniert eine Störung der Stromversorgung oder beeinflusst einzelne Systeme, ohne die der ordnungsgemäße Betrieb nicht möglich ist.
- Er meldet sich mit seinen Rechten an, stellt dabei fest, dass ein Gruppenrecht falsch konfiguriert ist und er hierüber seine Rechte ausweiten kann.
- Über diese Priviliegieneskalation und Lateral Movement über die Einzelsysteme der Edge-Komponente erhält er weitere Rechte auf der Edge-Komponente und stört so die Alarmierung oder ändert Protokollierungsereignisse, die Rückschlüsse auf ihn zulassen.

5.4.4.2 Handlungsempfehlungen

Um solche Angriffe zu erschweren, frühzeitig zu erkennen und die Auswirkungen gering zu halten, können folgende Maßnahmen umgesetzt werden:

- Es sollte ein Gebäudeschutz umgesetzt werden. Hierzu zählt eine Zutrittskontrolle zu Räumen oder Gebäuden mit schützenswerten Geräten. Räume, die Geräte enthalten, die besonders geschützt werden müssen, sollten zusätzlich überwacht werden. Ein unberechtigter Zutrittsversuch sollte aufgezeichnet und die Aufzeichnung ausgewertet werden.
- Anwendungen in der Edge-Komponente sollten auf abnormales Verhalten kontrolliert und automatische Alarmierungen durchgeführt werden. Hierzu zählt, relevante Protokollierungsdaten regelmäßig automatisiert auszuwerten, um den Befall von Schadsoftware rechtzeitig zu erkennen.
- Wenn mehrere Anwendungen auf einer Edge-Komponente parallel betrieben werden, sollten sie ähnlich wie in der Cloud stark voneinander (beispielsweise durch Netzsegmentierung und Berechtigungsmanagement) isoliert werden. Durch Ressourcenlimits und/oder Vergeben von Priorisierungen für die einzelnen Anwendungen kann verhindert werden, dass die Funktionsfähigkeit von einzelnen Diensten durch den erhöhten Ressourcenbedarf einer Fachanwendung eingeschränkt wird.
- Bei Bedarf sollte eine Sicherheitsüberprüfung von Personal und Dienstleistern angestrebt werden.
- Administratoren sollten eine intensive Schulung bekommen, da insbesondere das Berechtigungsmanagement sehr komplex und damit auch schwieriger zu bedienen sein kann. Die Rechtevergabe und Gruppenrichtlinien müssen sehr restriktiv vergeben werden.
- Mitarbeiter sollten bezogen auf solche Angriffe geschult werden.
- Der Ausfall der Edge-Komponente sollte über eine Alarmierung auffallen und zügig behoben werden.
- Ein Konzept zum Schutz vor Schadprogrammen sollte erstellt und Maßnahmen zur Isolation befallener Komponenten sollten bereitgestellt werden.
- Regelmäßige Updates von Softwarekomponenten sollten durchgeführt und hierfür die Administratoren sensibilisiert und verpflichtet werden.

5.4.4.3 Fazit / Netto-Risiken

Es wird ein Risiko darin gesehen, dass verschiedene Verfahren auf derselben Komponente sich gegenseitig beeinflussen können. Dies kann durch starke Isolationsmechanismen und gutes Identitäts- und Berechtigungsmanagement verringert werden. Durch Ressourcenmanagement kann verhindert werden, dass der Betrieb einer Fachanwendung durch einen ressourcenintensiven Betrieb einer anderen Anwendung gestört wird. Ein weiteres Risiko besteht darin, dass durch die Komplexität der Anwendung ein unzureichendes Berechtigungsmanagement umgesetzt wird und Personen/Entitäten der Zugriff auf Anwendungen erlaubt wird, für die sie keinen Zugriff haben sollten. Dieses kann durch umfangreiche Schulungen und ein sehr gut umgesetztes Berechtigungsmanagement weitestgehend auf Null reduziert werden.

6 Sicherheitsbetrachtungen für die praktische Umsetzung

6.1 Einleitung

Wie in den vorherigen Kapiteln beschrieben, sind einerseits die Möglichkeiten, wie Edge-Komponenten aufgebaut sind, sehr unterschiedlich. Andererseits kommen je nach Use Case noch umfangreiche Faktoren hinzu, welche die Sicherheitsbewertung darüber hinaus beeinflussen. Dies führt dazu, dass es nicht möglich ist, eine Sicherheitsempfehlung für alle möglichen Eventualitäten zu formulieren. Der Praxisleitfaden in diesem Kapitel soll Anwender unterstützen, Sicherheitsmaßnahmen für Edge-Komponenten und die Umgebung, in der sie eingesetzt werden, zu etablieren.

Hierbei wird davon ausgegangen, dass keine neuen IT-Systeme betrachtet werden. Edge-Komponenten bestehen aus bekannten IT-Einzelsystemen, Netzelementen und Cloud-Strukturen, deren Absicherung in zahlreichen Standards ausführlich beschrieben ist. Neu hinzu kommen Gefährdungen, die durch die Kombination der Einzelsysteme, der Vernetzung mit anderen Komponenten und dem Einsatzort entstehen. Diese entstehen vorangig durch eine hohe Vernetzung, eine hohe Komplexität, der Verarbeitung von teilweise außergewöhnlichen Datenformaten und dem teilweise ungewöhnlichen und/oder exponierten Einsatzort. Um diese Gefährdungen für eine Edge-Komponente in der Praxis zu erfassen und Maßnahmen dagegen zu etablieren, empfiehlt das BSI, dass die Fragen im nachfolgenden Kapitel beantwortet werden. Für eine detailliertere Betrachtung der IT-Sicherheit von Endgeräten wird auf den IT-Grundschutz und Endgeräte-spezifische Publikationen verwiesen.

Prinzipiell gilt bei Edge Computing ein ähnliches Shared Responsibility Modell wie beim Cloud Computing, wo häufig über ein Schichtenmodell betrachtet wird, wer die Verantwortung für welche Daten und IT-Systeme und damit auch deren Absicherung trägt. Wie beim Cloud Computing werden hier Dienste gemietet, so dass die Sicherheitsempfehlungen je nach eingesetztem Modell durch den Anbieter und/oder den Nutzer umgesetzt werden müssen. In einigen Anwendungen hat der Nutzer keinen Zugriff auf die Komponenten, in anderen kann der Anbieter die Funktionen zur Umsetzung nur anbieten und der Nutzer muss sie umsetzen. Prinzipiell ist es auch möglich, Edge Computing ohne externen Dienstleister aufzubauen, wobei hier keine Unterscheidung zu privaten Cloud-Systemen mehr besteht. In diesem Fall sind Nutzer und Anbieter das gleiche Unternehmen bzw. die gleiche Institution. Wenn bei Nutzung eines Dienstes Anwendungen für Dritte geschrieben werden, gibt es wieder Nutzende dieser Anwendung, was etwas missverständlich in einigen Szenarien sein kann. In diesem Kapitel sind ausdrücklich die Dienste-Anbieter und -Nutzer gemeint. Es sollte insgesamt beachtet werden, dass der Nutzer in der Planungs- und Beschaffungsphase schon darauf achten muss, Dienste auszuwählen, die ihm Funktionen zur Verfügung stellen, mit welchen er die für seinen Use Case erforderlichen Cyber-Sicherheitsempfehlungen umsetzen kann.

6.2 Praxisleitfaden

Wie auch bei Cloud Computing ist bei Edge Computing wichtig, die unterschiedlichen Phasen des Lebenszyklus [12] der Edge-Komponente aus Nutzersicht zu berücksichtigen. Hierbei ist wichtig, sich ausführlich mit den Phasen "Planung", "Beschaffung", "Einsatz" und "Ende" zu beschäftigen.

Abb. 8 Lebenszyklus einer Edge-Komponente aus Sicht des Anwenders

Bei der Planung des Einsatzes müssen eine Sicherheitsstrategie und Sicherheitskonzepte bzgl. des Einsatzes erarbeitet werden. Diese müssen in die Sicherheitsstrategie der Institution, welche die Edge-Komponenten einsetzen möchte, passen. Hierfür müssen sämtliche internen Vorschriften berücksichtigt werden, aber auch Compliance-Vorgaben, denen die Institution unterliegt (beispielsweise europäische sowie nationale gesetzliche Regulierungen wie IT-Sicherheitsgesetze, aber auch branchenspezifische Vorgaben und Standards). Auch für die zu verarbeitenden Daten sollten schon bei der Planung verschiedene Vorüberlegungen durchgeführt werden. Werden personenbezogene Daten für den Einsatz vorgesehen, so muss hier die DSGVO und deren korrespondierende Regelungen beachtet werden. Institutions-spezifische Überlegungen helfen den Schutzbedarf (Siehe BSI-Standard 200-2 IT-Grundschutzmethodik) festzulegen, der dabei hilft, notwendige Schutzmaßnahmen zu identifizieren. Hierbei unterstützen eine Gefährdungs- und Risikoanalyse. Im IT-Grundschutz werden Elementargefährdungen angegeben, die als Ausgangspunkt für die Gefährdungsanalyse dienen können. Bei der Beschaffung sollte nicht nur Wert daraufgelegt werden, dass die gewünschten Funktionen für die Ausführung zur Verfügung stehen, sondern auch Möglichkeiten vorliegen, die Daten nach dem festgelegten Schutzbedarf zu schützen. Ein Hinweis über die Güte der Sicherheitsfunktionen liefern Compliance-Nachweise oder Sicherheitszertifikate. Wie beim Cloud Computing können auch beim Edge Computing über Verträge mit dem Anbieter je nach Schutzbedarf mehr oder weniger umfangreiche Schutzmaßnahmen integriert werden, beispielsweise, ob ein Backup in den Edge-Komponenten selbst vorgehalten wird oder noch in eine Cloud gespiegelt wird. Auch wie umfangreich Auditfunktionen zum Einsatz kommen, kann je nach Schutzbedarf variiert werden. Während des Betriebs muss sichergestellt sein, dass die zur Verfügung stehenden Schutzmaßnahmen auch gut genutzt werden. Hierzu sind gut geschultes Personal, aber auch versierte Anwender notwendig. Je nach Komponente gibt es spezielle Migrationsverfahren, mit denen die Daten in die Komponente übertragen werden können oder, wenn Sensoren und Aktoren angeschlossen werden sollen, muss gegebenenfalls durch Proxys oder Wandler sichergestellt werden, dass die Protokolle sicher verarbeitet werden können. Vor Einsatz sollten auch schon Überlegungen stattfinden, wie die Daten bei einem möglichen Ende der Nutzung bei Bedarf wieder aus der Edge-Komponente zurückmigriert werden können und ggf. so gelöscht werden, dass nach Rückgabe der Komponente keine Reste mehr auf den Systemen verbleiben.

In den folgenden Unterkapiteln werden zu all diesen Themen Fragen aufgelistet, die Anwender unterstützen sollen, Edge-Komponenten in der Praxis gut absichern zu können.

6.2.1 Planung und Beschaffung (PB)

Während dieser Phase finden Vorüberlegungen statt, welche Komponenten für den Einsatzzweck geeignet sind. Hierbei sollten nicht nur funktionale Überlegungen stattfinden, sondern auch geschaut werden, ob die einzusetzende Edge-Komponente ausreichend Sicherheitsfunktionen anbietet oder unterstützt, damit die Sicherheitsziele erreicht und die Vorgaben erfüllt werden können. Hierfür ist es gut, eine Bestandsaufnahme durchzuführen, um zu erfassen, welche Vorgaben umgesetzt werden müssen und welche Sicherheitseigenschaften die Edge-Komponente besitzen soll.

6.2.1.1 PB1 Governance und Compliance

Welche Unternehmensspezifischen Sicherheitsanforderungen sind vorhanden? Welche allgemeinen Vorgaben müssen erfüllt sein?

Wenn IT-Grundschutz in der Institution umgesetzt ist, liegen eine Sicherheitsstrategie, eine Sicherheitsleitlinie und ein Sicherheitskonzept vor. Wenn geplant ist, eine Edge-Komponente einzusetzen, sollte die Institution prüfen, was diese unternehmensspezifischen Sicherheitsanforderungen zum Einsatz von IT-Systemen beinhalten. Bei Edge-Komponenten gibt es die Möglichkeit, ganze fremdadministrierte Hardware- und Software-Komponenten, die in das eigene Netz integriert werden können, zu mieten. Es gibt reine Software-Komponenten, die auf eigener Hardware aufgesetzt werden können, oder Komponenten, die außerhalb des eigenen Netzes gehostet und angeboten werden. Je nachdem, was gemietet werden soll, muss geprüft werden, ob die Edge-Komponente in die unternehmensspezifischen Sicherheitsanforderungen integriert werden kann oder ob es hier Widersprüche gibt. Wenn beispielsweise keine fremdadministrierten Komponenten im eigenen Netz zugelassen sind, kann an dieser Stelle geprüft werden, ob es Mitigationsmaßnahmen gibt, wo ein Einsatz unter Einhaltung der Sicherheitsziele möglich bleibt, wie beispielsweise der Betrieb in einem separaten Netzsegment. Wenn die Ziele mit der ausgewählten Edge-Komponente nicht eingehalten werden können, dann kann möglicherweise nach einer anderen Komponente, wie beispielsweise einer Software-Komponente, gesucht werden, die dieselben Funktionen liefert, aber hardwaretechnisch unter der Kontrolle der Institution liegt.

Für den normalen IT-Betrieb müssen zusätzlich in jeder Institution abhängig vom Standort, der Branche und der Größe der Institution verschiedene Vorgaben eingehalten werden. Diese gelten auch uneingeschränkt für die Edge-Komponente. Auch wenn durch das Servicemodell ein Anbieter eine Teilverantwortung für die Systeme hat, behält der Anwender immer die Verantwortung für die Daten, die mit der Komponente verarbeitet werden und muss darauf achten, dass je nach Schutzbedarf oder bei personenbezogenen Daten stärkere oder schwächere Vorgaben umzusetzen sind. Um die Möglichkeiten und Auswirkungen von Supply-Chain-Angriffen zu verringern, kann durch so genannte Software Bill of Materials (SBOM) oder Hardware Bill of Materials (HBOM) eine Inventarliste mit Angaben zu den verwendeten Komponenten mit Versionsnummern erstellt werden, so dass bei Bekanntwerden von Schwachstellen schneller Mitigationsmaßnahmen eingeleitet werden können. Das BSI hat hierzu eine Technische Richtlinie [11] herausgegeben. Über den Cyber Resilience Act und NIS2 wird spätestens im Herbst 2024 die Umsetzung von diesbezüglichen Vorgaben für einige Unternehmen verpflichtend, bei entsprechenden nationalen Vorgaben schon früher. Um einen guten Schutz gegen Supply-Chain-Angriffe zu erhalten, ist die Einbeziehung von SBOMs und HBOMs zur Übersicht, welche Schwachstellen in Edge-Komponenten versteckt sein können, jedoch auch ohne Vorgabe hilfreich.

ID	Frage
PB1.1	Sind Richtlinien für den zulässigen Gebrauch und sicheren Umgang mit Assets sowie den sicheren Gebrauch und Betrieb von Informationssystemen erstellt worden?
PB1.2	Enthält die Edge-Komponente ausreichend Sicherheitsfunktionen, um alle IT-Sicherheitsanforderungen umzusetzen? Sind diese ausreichend dokumentiert? Insbesondere wird hier auf Sicherheitsfunktionen hingewiesen, die in Kapitel 6.2.2.3 "Gefährdungsanalyse und Absicherung" für den Einsatz der

ID	Frage
	Komponenten gefordert werden. Darüber hinaus müssen auch Maßnahmen nach IT-Grundschutz oder C5 umgesetzt werden, wenn sie zusätzlich zur Erfüllung der unternehmensspezifischen IT-Sicherheitsanforderungen benötigt werden.
PB1.3	Gibt es bei Einsatz der Edge-Komponente Widersprüche zu den allgemeinen IT-Sicherheitsanforderungen der Institution? Welche Mitigationsmaßnahmen gibt es?
PB1.4	Erfüllt die Edge-Komponente die allgemeinen IT-Sicherheitsziele der Institution? Welche Funktionen der Edge-Komponente können dafür eingesetzt werden? Können die Sicherheitsziele durch äußere Maßnahmen hergestellt werden, wenn die Edge-Komponente keine geeigneten Sicherheitsfunktionen liefert oder wenn das Schutzziel es erfordert, eigene Maßnahmen zu nutzen (Beispielsweise Verschlüsselung mit eigenen Schlüsseln)?
PB1.5	Müssen Geheimschutzanforderungen umgesetzt werden? Was muss die Edge-Komponente dafür für Funktionen besitzen? Sprechen Geheimschutzaspekte gegen die Nutzung einer bestimmten Edge-Komponente? Können die Geheimschutzziele auch durch äußere Maßnahmen umgesetzt werden, wenn dies erforderlich ist?
PB1.6	Welche IT-Sicherheitsfunktionen werden für die Edge-Komponente angeboten? Welche Zusatzfunktionen, die für die Erfüllung der Ziele oder Pflichten benötigt werden, können vertraglich hinzugebucht werden (Beispielsweise Erarbeitung einer Service-Definition oder Vorgaben an die Portabilität, insbesondere die Rückgabe der Daten des Nutzers sollten vertraglich festgehalten und die Pflichten des Edge-Anbieters und des Nutzers definiert werden.)?
PB1.7	Muss die DSGVO angewendet und umgesetzt werden? Welche Möglichkeiten bietet die Edge-Komponente zum Schutz meiner Daten? Ist die Edge-Komponente von einem Anbieter eines anderen Landes, welches den Anbieter über gesetzliche Regelungen auffordern kann, Daten auf Komponenten herauszugeben?
PB1.8	Welche IT-Sicherheitsvorgaben müssen für den Einsatz der Edge-Komponente beachtet werden? Sind die Kriterien des C5 erfüllt? Werden ausreichende IT-Sicherheitsfunktionen angeboten, um IT-Grundschutz umzusetzen?
PB1.9	Welche Aspekte der IT-Sicherheitsgesetze müssen für den Einsatz der Edge-Komponente beachtet werden? Wird die Edge-Komponente in einer kritischen Infrastruktur eingesetzt? Welche Regelungen müssen beachtet werden? Werden ausreichende IT-Sicherheitsfunktionen angeboten, um diese Regelungen zu beachten? Wie kann bei Bedarf Ausfallsicherheit hergestellt werden?
PB1.10	In welcher Branche soll die Edge-Komponente eingesetzt werden? Gibt es hier branchenspezifische Vorgaben (Bsp. Dora im Finanzwesen oder Mindeststandards in Bundesbehörden), die eingehalten werden müssen? Werden ausreichende IT-Sicherheitsfunktionen angeboten, um diese Vorgaben einzuhalten?
PB1.11	Welche IT-Sicherheitszertifikate und Testierungen hat die Edge-Komponente? Welche Aussagen für die Absicherung der in der Komponente enthaltenen Systeme werden hierdurch erhalten?
PB1.12	Enthält die Edge-Komponente Software von Drittanbietern? Gibt es hierzu eine Auflistung (SBOM, HBOM), welche Anwendungen eingesetzt werden und welcher Softwarestand verwendet wurde? Werden bei der Komponente veraltete Versionen eingesetzt?

6.2.1.2 PB3 Einsatzort

Wo liegt der Einsatzort?
Es gibt unterschiedliche Gefährdungen je nach Einsatzort. Bei der Vielzahl der Use Cases, bei denen Edge-Komponenten eingesetzt werden können, gibt es sehr unterschiedliche Anforderungen an die Absicherung. Der Einsatz auf einer Bohrinsel hat andere Anforderungen als der Einsatz bei der Verkehrssteuerung oder in einem Unternehmensnetz.

ID	Frage
PB3.1	Wird die Komponente auf der inneren Edge-Ebene eingesetzt? Muss sie in einem separaten Netz eingesetzt werden?
PB3.2	Welche Schutzmaßnahmen werden aufgrund des Einsatzortes benötigt? Ist die Komponente durch das Gebäude geschützt? Ist die Komponente durch unberechtigte Personen zu erreichen?
PB3.3	Wird die Komponente auf der äußeren Edge-Ebene eingesetzt? Wie ist sie geschützt? Was muss noch an Schutzmaßnahmen hinzugefügt werden, um die Sicherheitsziele für die Daten zu erreichen?
PB3.4	Ist die Komponente in eine Basisstation eines Funknetzes integriert? Wie ist sie geschützt? Was muss noch an Schutzmaßnahmen hinzugefügt werden, um die Sicherheitsziele für die Daten zu erreichen?
PB3.5	Ist die Komponente in ein Endgerät integriert? Wie ist sie geschützt? Was muss noch an Schutzmaßnahmen hinzugefügt werden, um die Sicherheitsziele für die Daten zu erreichen?
PB3.6	Handelt es sich um eine exponiert stehende Komponente oder ist die Komponente durch ein Gebäude geschützt? Ist die Komponente durch unberechtigte Personen zu erreichen? Was muss an Schutzmaßnahmen hinzugefügt werden, um die Sicherheitsziele für die Daten zu erreichen?

6.2.1.3 PB4 Vernetzungsgrad

Wie hoch ist der Vernetzungsgrad?

Edge-Komponenten zeichnen sich durch einen hohen Grad der Vernetzung aus. Sie sind oft mit einer Vielzahl von Sensoren und Aktoren verbunden und häufig auch mit anderen Edge-Komponenten und/oder Cloud-Systemen. Durch diese hohe Vernetzung ergeben sich Gefährdungen für die Daten und Anwendungen, die in den Edge-Komponenten verarbeitet werden. Es entsteht aber auch in manchen Fällen für die angeschlossenen Endgeräte ein höheres Risiko, da die Endgeräte ohne die Edge-Komponente eventuell nicht so weitläufig vernetzt wären. Hierdurch kann unter Umständen ein weitreichender Schaden entstehen.

ID	Frage
PB4.1	Wie viele Endgeräte sind angeschlossen? Sind die Endgeräte über die Edge-Komponente miteinander gekoppelt? Wie können Angriffe auf die Edge-Komponente und ggf. auf angeschlossene Endgeräte verhindert werden, damit einem Großausfall der Endgeräte entgegengewirkt wird? Sind die Daten, die von den Endgeräten und zurück übertragen werden, ausreichend vor Manipulation und Verlust geschützt?
PB4.2	Wie viele weitere Edge-Komponenten sind über die Edge-Komponente angeschlossen? Sind diese alle auf einer Ebene (innere/äußere Edge-Ebene)? Wie können Angriffe auf die Edge-Komponente und ggf. auf angeschlossene Endgeräte verhindert werden, damit ein Großausfall der Edge-Komponenten entgegengewirkt wird? Sind die Daten, die zwischen den Komponenten übertragen werden, ausreichend vor Manipulation und Verlust geschützt?

ID	Frage
PB4.3	Ist die Edge-Komponente an eine oder mehrere Clouds angeschlossen? Sind die Daten, die in die Cloud und zurück übertragen werden, ausreichend vor Manipulation und Verlust geschützt?

6.2.2 Einsatz (EZ)

Beim Einsatz müssen die Sicherheitsfunktionen so eingesetzt werden, dass die Sicherheitsziele erreicht und die Vorgaben erfüllt werden. Um Daten mit der Edge-Komponente verarbeiten zu können, müssen die Daten möglicherweise in ein von der Edge-Komponente gefordertes Format überführt werden. Wenn die Sensoren oder Aktoren, mit denen Daten ausgetauscht werden, unsichere Protokolle anbieten, muss über Proxies oder Wandler dafür gesorgt werden, dass die Edge-Komponente, aber auch die Endgeräte und alle weiteren angeschlossenen Edge-Komponenten geschützt bleiben. Wenn die Komponente sehr stark vernetzt ist oder an einem exponierten Einsatzort eingesetzt wird, so erhöht sich die Möglichkeit von Angriffen. Hierfür müssen spezielle Maßnahmen umgesetzt werden. Zur schnellen Erkennung von IT-Sicherheitsvorfällen müssen eine gute Protokollierung aufgesetzt und Maßnahmen ergriffen werden, dass die Protokollierung regelmäßig ausgewertet wird. Zur schnellen Behebung von Schwachstellen muss gewährleistet sein, dass schnell Updates oder Mitigationsmaßnahmen zur Verfügung stehen.

6.2.2.1 Schulung und Dokumentation

Sind Anwender und Administratoren in der Lage die Edge-Komponente sicher zu bedienen?
Das Vorhandensein von Sicherheitsfunktionen stellt noch nicht sicher, dass diese auch optimal genutzt werden. Um die bestmögliche Absicherung umzusetzen, bedarf es einer guten Dokumentation und der Schulung aller Beteiligten.

ID	Frage
EZ1.1	Sind die Verantwortlichkeiten genau identifiziert und dokumentiert?
EZ1.2	Gibt es Anwenderdokumentation oder -schulungen? Sind die Anwender ausreichend informiert, um die Edge-Komponente sicher zu bedienen?
EZ1.3	Gibt es Administratordokumentation oder -schulungen? Sind die Administratoren ausreichend informiert, um die Edge-Komponente sicher zu bedienen, wie sie mit den verarbeiteten Daten umgehen müssen, was bei der aktuellen Bedrohungslage unternommen werden muss und wie bei Sicherheitsvorfällen vorgegangen werden muss?

6.2.2.2 Migration der Daten

Welche Vorkehrungen sind vor der Betriebsphase zu treffen, um Daten mit der Edge-Komponente sicher verarbeiten zu können?

Vor dem eigentlichen Betrieb der Edge-Komponente werden Verbindungen geschaffen, über die Daten in die Edge-Komponente fließen sollen. Dieser Punkt gilt nicht nur vor der Betriebsphase sondern auch darüber hinaus. Er wird in den Tabellen des nächsten Unterkapitels erneut behandelt, da bei dem Betrieb von vielen Edge-Komponenten kontinuierlich neue Datenquellen angeschlossen werden.

ID	Frage
EZ2.1	Welches Datenformat wird verarbeitet? Muss das Format, das von anderen Komponenten oder den Endgeräten geliefert wird, angepasst werden? Wie kann die Integrität der Daten sichergestellt werden?
EZ2.2	Welche Protokolle werden bei der Übertragung genutzt? Müssen die Daten verschlüsselt übertragen werden?

6.2.2.3 Gefährdungsanalyse und Absicherung

Bei der Absicherung der Edge-Komponente wird davon ausgegangen, dass keine neuen IT-Systeme betrachtet werden. Edge-Komponenten bestehen aus bekannten IT-Einzelsystemen, Netzelementen und Cloud-Strukturen, deren Absicherung in zahlreichen Standards ausführlich beschrieben ist. Neu hinzu kommen Gefährdungen, die durch die Kombination der Einzelsysteme, der Vernetzung mit anderen Komponenten und des Einsatzortes entstehen. Zusätzlich muss beim Einsatz geschaut werden, welche Einzelelemente der Edge-Komponente in der Verantwortung des Anwenders stehen.

Dies geschieht zweistufig. Zunächst muss eine Betrachtung der Einzelsysteme der Komponente durchgeführt werden und dann ein Blick von außen auf die Edge-Komponente geworfen werden, um allgemeine Gefährdungen durch das Zusammenspiel der Einzelsysteme, die Vernetzung und den Einsatzort zu identifizieren.

Für die Absicherung der Einzelsysteme müssen folgende Fragen betrachtet werden:

ID	Frage
EZ3.1	Welche Einzelsysteme, Netzelemente und Cloud-Strukturen können identifiziert werden? Handelt es sich um eine reine Software-Komponente? Welche zusätzlichen IT-Systeme müssen noch für den Betrieb der Komponente vom Anwender hinzugefügt werden?
EZ3.2	Welche Absicherung muss für die für den Betrieb identifizierten, hinzugefügten Einzelsysteme und Netzelemente nach IT-Grundschutz noch umgesetzt werden?
EZ3.3	Welche korrespondierenden Kriterien, die von Kunden umgesetzt werden müssen, können nach C5 identifiziert werden? Was muss hiervon umgesetzt werden, damit die vorher festgelegten Sicherheitsziele erreicht werden können?

Im Folgenden werden die für Edge-Komponenten neu hinzukommenden Gefährdungen genauer betrachtet. Sie entstehen durch die Kombination der Komponenten, Einzelsysteme und Netzelemente. Hauptsächlich entstehen die Gefährdungen durch exponierte Einsatzorte in den mannigfaltigen Use Cases, die hohe Komplexität der Komponenten oder die sehr weitreichende Vernetzung. Es wird von der bisher verwendeten Frageform abgewichen und intensiv auf diese Edge-spezifischen Besonderheiten eingegangen. Bei den im Anschluss an die Gefährdungskapitel folgenden Unterkapitel behandelten Fragestellungen handelt es sich wieder um Fragestellungen, die aus anderen Infrastrukturen und Systemen bekannt sind, daher wird dann wieder zu der Frageform zurückgekehrt.

Es werden hier die aus Sicht des BSI relevantesten Gefährdungen beschrieben, die zum aktuellen Zeitpunkt für Edge Computing ersichtlich sind. Es wird das Risiko beschrieben, welches durch die Gefährdungen besteht und welche Sicherheitsempfehlungen den Risiken entgegengesetzt werden können. Grundsätzlich sind die Gefährdungen, Risiken und Sicherheitsempfehlungen vergleichbar zu denen von Cloud-Systemen.

Die meisten der hier aufgeführten Gefährdungen sind bei Edge Computing durchgängig vorhanden. Die sich daraus ergebenden Risiken sind aber stark durch das Einsatzszenario (Schutzbedarf und Eintrittswahrscheinlichkeit bspw. durch Exponiertheit und der Angreiferklassifikation) bedingt. Insgesamt werden an dieser Stelle die Gefährdungen, Risiken und Sicherheitsempfehlungen nur sehr allgemein beschrieben, da je nach Use Case sehr unterschiedliche Ausprägungen der Gefährdungen und Risiken entstehen. Dies muss in der Praxis weiter ausgearbeitet werden.

Der besseren Übersicht halber werden die Gefährdungen, Risiken und Sicherheitsempfehlungen weiter unten tabellarisch dargestellt. Hierbei muss generell unterschieden werden, ob die innere oder die äußere Edge-Ebene betrachtet wird. Da die äußere Ebene außerhalb des Endgerätenetzes liegt, liegen hier für den Anwender oft nur eingeschränktere Möglichkeiten der Absicherung vor als wenn die Komponenten im Endgerätenetz eingesetzt werden. Hier müssen Absicherungen durch den Anbieter erfolgen. Absicherungen, die durch den Anbieter erfolgen müssen, wurden bei der Planungs- und Beschaffungsphase stärker

betrachtet, so dass in der nachfolgenden Tabelle vorrangig die Absicherungen durch den Anwender beschrieben sind.

Die nachfolgenden Tabellen sind wie folgt zu lesen. In der ersten Spalte sind die Gefährdungen als Schlagwörter, in Klammern folgt jeweils ein Bezug zu der Liste der "Elementaren Gefährdungen" aus dem IT-Grundschutz und darunter eine kurze Erläuterung des möglichen Angriffsszenarios oder des vorliegenden Mangels beim Einsatz der Edge-Komponente. Die Spalte Risiko beschreibt, welche Sicherheitsziele durch die Gefährdungen verletzt werden. Sie kann in einer Risikoanalyse unterstützen, Entscheidungen zu treffen, welche Sicherheitsmaßnahmen am Ende umgesetzt werden. Hierzu müssen der Schutzbedarf, der an dieser Stelle nicht betrachtet wird, und die Besonderheiten des Uses Cases mit berücksichtigt werden. Die Sicherheitsempfehlungen sind hier getrennt nach innerer und äußerer Edge-Ebene aufgebaut. Für Komponenten, die in die Netztechnologie integriert sind, gelten die Empfehlungen der äußeren Edge-Ebene und für Komponenten, die in Endgeräte integriert sind, die der inneren Edge-Ebene. Das Anmerkungsfeld enthält Erläuterungen zu möglichen Auswirkungen und Aspekten, die durch die Struktur der Tabelle eventuell zu ungenau beschrieben sind.

6.2.2.3.1 Organisatorisches/Rahmenbedingungen

Gefährdungen	Risiko	Sicherheitsempfehlungen innere Edge-Ebene	Sicherheitsempfehlungen äußere Edge-Ebene	Anmerkung
Mangelnde Interoperabilität (Fehlplanung oder fehlende Anpassung) Mangelnde Interoperabilität zwischen unterschiedlichen Edge-Systemen kann durch den Einsatz unterschiedlicher Hersteller und proprietärer Produkte entstehen.	hohe Kosten Verfügbarkeit gestört	Nutzen standardisierter Schnittstellen, Formate und Funktionen Konzeption eines Lifecycle Management mit Notfallstrategie.	Nutzen standardisierter Schnittstellen, Formate und Funktionen Konzeption eines Lifecycle Management mit Notfallstrategie.	Als Auswirkungen können beispielsweise eine Abhängigkeit von Herstellern, ein so genannter Vendor Lock-In oder Datenverlust entstehen.
Unklarheiten über die Pflichten (Shared Responsibility Model, Verstoß gegen Gesetze oder Regelungen) Ein Verstoß gegen Gesetze und Regelungen kann entstehen, wenn die Pflichten von Anbieter und Nutzer (shared responsibility) nicht vollständig geklärt sind, zum Beispiel durch die ungenügende oder missverständliche Beschreibung von Verantwortungsbereichen, Aufgaben, Leistungsparametern oder Aufwänden. Dadurch besteht die Gefahr, dass Anforderungen an einen sicheren Betrieb durch den Betreiber u.U. nicht gewährleistet sind. Edge-Komponenten, sind u.U. in ihrer Standardausprägung nicht sicher konfiguriert, des Weiteren müssen auch Geräte bezüglich ihrer Firmware, Software etc. verwaltet und gepflegt werden.	hohe Kosten Schaden der Reputation Verlust von Integrität, Vertraulichkeit und Verfügbarkeit strafrechtliche Konsequenzen	Klare Identifikation und Dokumentation von Schnittstellen/ Verantwortlichkeiten/ Aufgaben/ Zuständigkeiten zwischen Anbieter und Nutzer durch genaue Verträge, Abgrenzung der Verantwortungsbereiche	Klare Identifikation und Dokumentation von Schnittstellen/ Verantwortlichkeiten/ Aufgaben/ Zuständigkeiten zwischen Anbieter und Nutzer durch genaue Verträge, Abgrenzung der Verantwortungsbereiche	Jegliche unerwünschte Zustände oder Angriffe durch Dritte können durch ungeeignetes oder unzureichendes Management eintreten.
Unklarheiten über Compliance und Governance (Verstoß gegen Gesetze oder Regelungen) Mögliche Gefährdung durch Nichtbeachtung von Vorgaben, da	hohe Kosten Schaden der Reputation Verlust von Integrität,	Sensibilisierung der Mitarbeiter, insbesondere in Bezug auf die gegebenenfalls neue Rolle als Dienst-Nutzender	Sensibilisierung der Mitarbeiter, insbesondere in Bezug auf die gegebenenfalls neue Rolle als Dienst-Nutzender	Jegliche unerwünschte Zustände oder Angriffe durch Dritte können durch ungeeignetes oder unzureichendes Management eintreten.

Gefährdungen	Risiko	Sicherheitsempfehlungen innere Edge-Ebene	Sicherheitsempfehlungen äußere Edge-Ebene	Anmerkung
Compliance / Governance nicht bekannt sind. Einsatz von Edge-Komponenten zur Verarbeitung von Daten, ohne dass ausreichende Schutzmaßnahmen für die Erhaltung der vorliegenden Sicherheitsziele bestehen.	Vertraulichkeit und Verfügbarkeit strafrechtliche Konsequenzen	Umsetzung aktueller Informationen zur sicheren Konfiguration und Beobachtung der Informationen über bekannte Schwachstellen des Edge-Dienstes, Nutzung geeigneter Mechanismen zur Fehlerbehandlung und Protokollierung sowie zur Authentisierung und Autorisierung von Benutzern der (Edge-)Nutzer. Sichere Nutzung der Funktionen, die unterstützen Compliance/Governance umzusetzen	Umsetzung aktueller Informationen zur sicheren Konfiguration und Beobachtung der Informationen über bekannte Schwachstellen des Edge-Dienstes, Nutzung geeigneter Mechanismen zur Fehlerbehandlung und Protokollierung sowie zur Authentisierung und Autorisierung von Benutzern der (Edge-)Nutzer. Sichere Nutzung der Funktionen, die unterstützen Compliance/Governance umzusetzen	
Zugriff auf geteilte Ressourcen durch juristisch unterschiedliche Rollen (Unberechtigte Nutzung oder Administration von Geräten und Systemen) Im Gegensatz zur inneren Edge-Ebene gibt es in der äußeren Edge-Ebene oft mehrere juristisch unterschiedliche Rollen, die sich eine Plattform teilen. Hierdurch kann ein Zugriff auf geteilte Ressourcen durch juristisch unterschiedliche Rollen erfolgen	Verlust von Integrität, Vertraulichkeit und Verfügbarkeit	Meist greift hier nur ein Endanwender zu, Greifen aber doch mehrere Endanwender zu, sollte eine Trennung von Verantwortlichkeiten / Aufgaben auf Basis der Risikobeurteilung erfolgen Ist eine Trennung nicht möglich, sollte die entsprechende Tätigkeit geeignet überwacht werden	Trennung von Verantwortlichkeiten / Aufgaben auf Basis einer Risikobeurteilung. Ist eine Trennung nicht möglich, sollte die entsprechende Tätigkeit geeignet überwacht werden Umsetzung Berechtigungsmanagement/ IAM-Maßnahmen nach Zero Trust-Prinzipien / Assume Breach Ansatz, insbesondere Beachtung der "Least Privilege"- und "Need to Know"-Prinzipien, Einsatz von MFA sowie regelmäßige oder anlassbezogene Prüfung und Anpassung von Berechtigungen (Identity Lifecycle Management) Je nach Use Case und Schutzbedarf sollten weitere Maßnahmen wie (starke) Verschlüsselung entsprechend dem Stand der Technik sowie die Verwendung von Mechanismen wie Schlüsselrotation und bei Bedarf eigenen Public Key Infrastrukturen	Es kann bei unzureichender Abgrenzung eine gegenseitige Beeinflussung entstehen, die die Verfügbarkeit beeinträchtigt. Durch Zugriffe auf Inhalte von Dritten können Vertraulichkeit und Integrität geschädigt werden Der Anwender ist verantwortlich, seine Daten nach Stand der Technik zu schützen. Wenn Daten mit höherem Schutzbedarf verarbeitet werden sollen, so kann der Anwender über selbst kontrollierten Maßnahmen neben der Reduzierung des Risikos, dass Daten an Dritte abfließen auch das Risiko des unzulässigen Datenabflusses an den Provider minimieren.

Gefährdungen	Risiko	Sicherheitsempfehlungen innere Edge-Ebene	Sicherheitsempfehlungen äußere Edge-Ebene	Anmerkung
			(PKI) für das Verschlüsseln der Daten, die zwischen Entitäten ausgetauscht werden oder physische Isolation (Einsatz eines HSM als Trusted Computing Base (TCB) oder Trusted Execution Environment (TEE)) als vertrauenswürdige Basis für die Aufbewahrung und den Einsatz kryptographischer Schlüssel bzw. als vertrauenswürdige Umgebung für die Ausführung von Code), sofern möglich, umgesetzt werden.	

6.2.2.3.2 Infrastruktur/Architektur

Gefährdung	Risiko	Sicherheitsempfehlungen innere Edge-Ebene	Sicherheitsempfehlungen äußere Edge-Ebene	Anmerkung
Physische Exposition (Ausfall oder Störung der Edge-Komponente, der Netzanbindung oder der Stromversorgung sowie möglicher Diebstahl, Zerstörung oder Verlust von Komponenten und Sabotage) Edge-Komponenten werden oft an weniger abgesicherten oder schlechter an übliche Infrastrukturen angebundenen Orten platziert, als dass dies bspw. in einem abgesicherten Cloud-Rechenzentrum der Fall wäre. Durch diese pysische Exposition bzw. den teilweise unüblichen Einsatzort entsteht die Möglichkeit, dass Dritte Zugriff auf die Komponente erhalten, diese stören oder zerstören, Zugriff auf die Daten erhalten oder der Netzwerkverkehr abgehört oder gestört werden kann.	Verlust von Integrität, Vertraulichkeit und Verfügbarkeit	Physische Absicherung (insbesondere, soweit im spezifischen Use Case möglich, in Form des Perimeterschutzes sowie des Schutzes vor Feuer, Rauch und Ausfall der Versorgungseinrichtungen), Redundanzen (ggf. zwei Standorte, die sich einander Betriebsredundanz geben), Objektschutz, Überwachung der Betriebs- und Umgebungsparameter Überprüfung der Qualifikation und Vertrauenswürdigkeit der Zugriffs-Berechtigten unter Beachtung der lokalen Gesetzgebung. Falls der Schutzbedarf dies erforderlich macht,	Physische Absicherung (insbesondere, soweit im spezifischen Use Case möglich, in Form des Perimeterschutzes sowie des Schutzes vor Feuer, Rauch und Ausfall der Versorgunseinrichtungen), Redundanzen (ggf. zwei Standorte, die sich einander Betriebsredundanz geben), Objektschutz, Überwachung der Betriebs- und Umgebungsparameter Überprüfung der Qualifikation und Vertrauenswürdigkeit der Zugriffs-Berechtigten unter Beachtung der lokalen Gesetzgebung. Falls der Schutzbedarf dies erforderlich macht, sollte die Überprüfung in Form einer Sicherheitsüberprüfung erfolgen Berechtigungsmanagement/ IAM-Maßnahmen nach Zero Trust-Prinzipien	Nach dem hier verwendeten Modell ist der Nutzer für einige der Maßnahmen auf der inneren Edge-Ebene zuständig, da die Komponenten in seinem Netz liegen und auf der äußeren meist der Anbieter. In verschiedenen Use Cases verschwimmen die klaren Trennungen, so dass hier eine Use Case-spezifische Betrachtung durchgeführt werden muss.

Gefährdung	Risiko	Sicherheitsempfehlungen innere Edge-Ebene	Sicherheitsempfehlungen äußere Edge-Ebene	Anmerkung
		sollte die Überprüfung in Form einer Sicherheitsüberprüfung erfolgen Berechtigungsmanagement/ IAM-Maßnahmen nach Zero Trust-Prinzipien / Assume Breach Ansatz, insbesondere Beachtung der "Least Privilege"- und "Need to Know"-Prinzipien, Einsatz von MFA sowie regelmäßige oder anlassbezogene Prüfung und Anpassung von Berechtigungen (Identity Lifecycle Management) Maßnahmen zur Datensicherheit (Verschlüsselung, Separation,...). Für die Verschlüsselung verwendete private Schlüssel sind ausschließlich dem Nutzer bekannt. Je nach Schutzbedarf sollten die verwendeten Mechanismen und Schlüssellängen vertraglich geregelt werden. Dort, wo die Nutzer eigene Verschlüsselungsmechanismen verwenden, sollten sie ein geeignetes Schlüsselmanagement sicherstellen Starke Verschlüsselung und Authentifizierung entsprechend dem Stand der Technik, mindestens bei dem Transport von Daten. Je nach Schutzbedarf sollten die verwendeten Mechanismen und Schlüssellängen vertraglich geregelt werden	/ Assume Breach Ansatz, insbesondere Beachtung der "Least Privilege"- und "Need to Know"-Prinzipien, Einsatz von MFA sowie regelmäßige oder anlassbezogene Prüfung und Anpassung von Berechtigungen (Identity Lifecycle Management) Maßnahmen zur Datensicherheit (Verschlüsselung, Separation,...). Für die Verschlüsselung verwendete private Schlüssel sind ausschließlich dem Nutzer bekannt. Je nach Schutzbedarf sollten die verwendeten Mechanismen und Schlüssellängen vertraglich geregelt werden. Dort, wo die Nutzer eigene Verschlüsselungsmechanismen verwenden, sollten sie ein geeignetes Schlüsselmanagement sicherstellen Starke Verschlüsselung und Authentifizierung entsprechend dem Stand der Technik, mindestens bei dem Transport von Daten. Je nach Schutzbedarf sollten die verwendeten Mechanismen und Schlüssellängen vertraglich geregelt werden Etablierung von Mechanismen zum Manipulationsschutz, die nur temporär und nur durch authorisiertes Personal (z.B. im Rahmen von Wartungen) deaktiviert werden können. Funktionen müssen auch dann funktionsfähig bleiben, wenn keine aktive Verbindung zu den	

Gefährdung	Risiko	Sicherheitsempfehlungen innere Edge-Ebene	Sicherheitsempfehlungen äußere Edge-Ebene	Anmerkung
		Etablierung von Mechanismen zum Manipulationsschutz, die nur temporär und nur durch authorisiertes Personal (z.B. im Rahmen von Wartungen) deaktiviert werden können. Funktionen müssen auch dann funktionsfähig bleiben, wenn keine aktive Verbindung zu den übergeordneten Verwaltungsdiensten (bspw. Konfigurationen, die in der Cloud vorgehalten werden) besteht. Diese Dienste können durch Redundanzen auf den Edge-Ebenen und die Zusammenarbeit zwischen unterschiedlichen Edge-Komponenten durchgängig verfügbar gemacht werden	übergeordneten Verwaltungsdiensten (bspw. Konfigurationen, die in der Cloud vorgehalten werden) besteht. Diese Dienste können durch Redundanzen auf den Edge-Ebenen und die Zusammenarbeit zwischen unterschiedlichen Edge-Komponenten durchgängig verfügbar gemacht werden	

6.2.2.3.3 Kommunikation/Daten/Vernetzung

Gefährdung	Risiko	Sicherheitsempfehlungen innere Edge-Ebene	Sicherheitsempfehlungen äußere Edge-Ebene	Anmerkung
Kein oder unzureichender Schutz bei Übermittlung von Daten (Fehlplanung oder fehlende Anpassung) Wenn kein oder nur ein unzureichender Schutz bei der Übermittlung von Daten umgesetzt wird, kann es zu Zugriffsmöglichkeiten durch Dritte kommen	Verlust von Integrität, Vertraulichkeit und Verfügbarkeit	Einsatz von Endgeräten, die über standardisierte Schnittstellen verfügen.	Es wird davon ausgegangen, dass auf der äußeren Edge-Ebene grundsätzlich nur standardisierte Schnittstellen eingesetzt werden, da diese oft nicht direkt mit Endgeräten kommunizieren. Sollte dies doch der Fall sein, wird der Einsatz von Geräten, die über standardisierte Schnittstellen verfügen empfohlen.	Wenn bei der Übermittlung der Daten von den Endgeräten zur inneren Edge-Ebene bzw. von innerer Edge-Ebene zur äußeren Edge-Ebene nicht dem Schutzbedarf entsprechend vor unberechtigtem Zugriff oder Manipulation geschützt werden, sind Anbieter und Nutzer beide in der Pflicht weitere Schutzmaßnahmen umzusetzen. Der Nutzer muss darauf achten, dass seine Endgeräte und

Gefährdung	Risiko	Sicherheitsempfehlungen innere Edge-Ebene	Sicherheitsempfehlungen äußere Edge-Ebene	Anmerkung
		Netzsegmentierung: Unterscheidung zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzen, Festlegung zugelassener interner und externer Kommunikation und Verbindungen, Überwachung der hergestellten Verbindungen Schutz der Netzperimeter durch Sicherheitsgateways, die basierend auf den Sicherheitsanforderungen des jeweiligen Use Cases konfiguriert sind und deren Protokolle automatisiert ausgewertet werden Auswahl von geeigneten Kommunikationsprotokollen, insbesondere Netz- und Anwendungsprotokollen Anbindung von nicht unterstützten Komponenten über Koppler/Proxy/Gateways Falls der Edge-Dienst SDN-Funktionalitäten anbietet, sollen SDN-Verfahren verwendet werden, die geeignet sind, die Vertraulichkeit der Nutzer-Daten sicherzustellen	Netzsegmentierung: Unterscheidung zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzen, Festlegung zugelassener interner und externer Kommunikation und Verbindungen, Überwachung der hergestellten Verbindungen Schutz der Netzperimeter durch Sicherheitsgateways, die basierend auf den Sicherheitsanforderungen des jeweiligen Use Cases konfiguriert sind und deren Protokolle automatisiert ausgewertet werden Auswahl von geeigneten Kommunikationsprotokollen, insbesondere Netz- und Anwendungsprotokollen Anbindung von nicht unterstützten Komponenten über Koppler/Proxy/Gateways Falls der Edge-Dienst SDN-Funktionalitäten anbietet, sollen SDN-Verfahren verwendet werden, die geeignet sind, die Vertraulichkeit der Nutzer-Daten sicherzustellen	Daten geschützt bleiben und der Anbieter, dass die Edge-Komponenten nicht angreifbar sind.
Zu hohe Komplexität (Fehlerhafte Nutzung oder Administration von Geräten und Systemen) Es besteht bei Edge-Komponenten eine sehr hohe Komplexität durch sehr viele Konfigurationsmöglichkeiten. Auch die vielen heterogenen Systeme, die innerhalb der Komponente verwendet oder angeschlossen werden, können zu	Verlust von Integrität, Vertraulichkeit und Verfügbarkeit	Sorgfältige Planung der Einbindung der Edge-Komponente in die IT unter Berücksichtigung mindestens der Anpassungen der Schnittstellen, des Administrationsmodells sowie des Datenmanagementmodells Einsatz eines standardisierten Änderungs- und Konfigurationsmanagements	Sorgfältige Planung der Einbindung der Edge-Komponente in die IT unter Berücksichtigung mindestens der Anpassungen der Schnittstellen, des Administrationsmodells sowie des Datenmanagementmodells Einsatz eines standardisierten Änderungs- und Konfigurationsmanagements	Der Einsatz eines standardisierten Änderungs- und Konfigurationsmanagements bedeutet, dass alle Veränderungen an Strukturen oder Konfiguration reproduzierbar durchgeführt und dokumentiert werden

Gefährdung	Risiko	Sicherheitsempfehlungen innere Edge-Ebene	Sicherheitsempfehlungen äußere Edge-Ebene	Anmerkung
zahlreichen Fehlfunktionen führen. Es besteht die Möglichkeit, dass veraltete Versionen im Einsatz sind und deren Schwachstellen ausgenutzt oder durch Konfigurationsfehler ungeplante Veränderungen durchgeführt werden.		Asset-Management, welches ein angemessenes Schutzniveau über den gesamten Lebenszyklus des Assets hinweg sicherstellt, etablieren. Assets sollten entweder automatisch oder durch die zuständige Person oder Gruppe inventarisiert werden.	Asset-Management, welches ein angemessenes Schutzniveau über den gesamten Lebenszyklus des Assets hinweg sicherstellt, etablieren. Assets sollten entweder automatisch oder durch die zuständige Person oder Gruppe inventarisiert werden.	
Hoher Vernetzungsgrad einer gestiegenen Anzahl an Geräten (Fehlfunktion von Geräten oder Systemen bzw. Überlastung und Ausfall) Durch die gestiegene Anzahl an Geräten in den einzelnen Schichten des Edge Computing (speziell auf der Endgeräteebene) entsteht eine große Menge an Daten, was dazu führen kann, dass die Menge der anfallenden Daten nicht verarbeitet werden kann, eine zu hohe Latenz entsteht und einzelne Komponenten ausfallen können. Aufgrund des hohen Vernetzungsgrades der Geräte können sich zudem Schadprogramme, von denen mindestens ein Gerät betroffen ist, schnell ausbreiten	Verlust von Verfügbarkeit und Integrität	Regelmäßige Kapazitätsplanung unter Nutzung von Prognosen zukünftiger Kapazitätsanforderungen durchführen und Kapazitätenverbrauch im Betrieb durch technische und organisatorische Maßnahmen überwachen (Capacity Management) Backup-Strategie zur Sicherung der Daten gemäß zuvor erhobener Anforderungen Systemspezifische Schutzmechanismen zur Erkennung und Beseitigung von Schadprogrammen sollten genutzt und automatisch überwacht werden Notfallstrategie, welche mindestens Zuständigkeiten und Kontaktpersonen, Regelungen hinsichtlich Datensicherung und Vorgaben zu redundant auszulegenden Management-Tools und Schnittstellensystemen inkludiert. Methoden zur Inkraftsetzung der Strategie sollten etabliert werden.	Capacity Management ist für die äußere Edge-Ebene weniger relevant, da hier in der Regel weniger Daten von Geräten anfallen. Backup-Strategie zur Sicherung der Daten gemäß zuvor erhobener Anforderungen Systemspezifische Schutzmechanismen zur Erkennung und Beseitigung von Schadprogrammen sollten genutzt und automatisch überwacht werden Notfallstrategie, welche mindestens Zuständigkeiten und Kontaktpersonen, Regelungen hinsichtlich Datensicherung und Vorgaben zu redundant auszulegenden Management-Tools und Schnittstellensystemen inkludiert. Methoden zur Inkraftsetzung der Strategie sollten etabliert werden	k.A.

Gefährdung	Risiko	Sicherheitsempfehlungen innere Edge-Ebene	Sicherheitsempfehlungen äußere Edge-Ebene	Anmerkung
Ausfall/Störung von Kommunikationsnetzen Durch Verbindungsstörungen oder Denial of Service Angriffe kann die Übertragung von Daten ausfallen oder zu langsam erfolgen. Im schlimmsten Fall können Daten verloren gehen, was die Integrität der Ergebnisse beeinflusst.	Verlust von Verfügbarkeit und Integrität	Zwischenspeicherung, Maßnahmen gegen DoS und andere Netz-basierte Angriffe sowie Einspeisung der Daten in ein SIEM, Konzeption von Fallbacklösungen für den Ausfall der Verbindung	Zwischenspeicherung, Maßnahmen gegen DoS und andere Netz-basierte Angriffe sowie Einspeisung der Daten in ein SIEM, Konzeption von Fallbacklösungen für den Ausfall der Verbindung	k.A.

6.2.2.4 Behebung von Schwachstellen, Detektion und Protokollierung

Wie werden Sicherheitsvorfälle erkannt und Schwachstellen behoben?

Zur schnellen Erkennung von IT-Sicherheitsvorfällen muss eine gute Protokollierung aufgesetzt werden. Es müssen Maßnahmen ergriffen werden, dass die Protokollierungsdaten regelmäßig ausgewertet werden. Zur schnellen Behebung von Schwachstellen muss gewährleistet sein, dass schnell Updates oder Mitigationsmaßnahmen zur Verfügung stehen.

ID	Frage
EZ4.1	Wurde ein Lifecycle-Management für Härtung, Updates und Patches etabliert? Wurde hierbei beachtet, dass eine Benachrichtigung der Nutzenden über die Art und den Umfang der Änderungen durch die Administratoren etabliert wurden (beispielsweise müssen bei Verwendung von Containern eventuell erneut Maßnahmen zu deren Absicherung getroffen werden (Härtung der Container, Erhaltung der Integrität des Container Stacks))?
EZ4.2	Werden für alle beteiligten Einzelsysteme automatisch Updates eingespielt? Wurden die Auswirkungen der Updates und Patches ausreichend überprüft und kontrolliert? Müssen gegebenenfalls für einige Systeme oder deren Komponenten manuell Updates eingespielt werden? Existieren für alle beteiligten IT-Systeme und Netzkomponenten Maßnahmen, um über Schwachstellen rechtzeitig informiert zu werden?
EZ4.3	Werden sicherheitsrelevante Ereignisse protokolliert?
EZ4.4	Werden die Protokolldaten bezüglich Anomalien und Sicherheitsvorfällen untersucht?
EZ4.5	Ist die Edge-Komponente an Intrusion Detektion- und Prevention-Systeme angeschlossen? Findet eine Erkennung von Schadsoftware statt?

6.2.3 Ende des Einsatzes (EX)

Bei Beendigung des Einsatzes, sollte sichergestellt sein, dass die in der Edge-Komponente enthaltenen Daten, Modelle und Ergebnisse von Berechnungen vom Anwender in andere Systeme übernommen werden können. Anschließend muss die Edge-Komponente bereinigt werden und die enthaltenen Daten nicht wiederherstellbar gelöscht werden.

6.2.3.1 Rückmigration von Daten

Welche Daten werden nach Ende der Nutzung der Edge-Komponente benötigt und wie können sie ohne Verluste in meine Systeme übertragen werden?

Bei Beendigung des Einsatzes, sollte sichergestellt sein, dass die in der Edge-Komponente enthaltenen Daten, Modelle und Ergebnisse von Berechnungen vom Anwender in andere Systeme übernommen werden können.

ID	Frage
EX3.1	Welche Daten werden nach Abschluss noch benötigt?
EX3.2	Welches Datenformat wird verarbeitet? Muss es auf das Format, dass von anderen Komponenten oder den Endgeräten geliefert wird, angepasst werden? Wie kann die Integrität bei der Übertragung der Daten sichergestellt werden?
EX3.3	Können eventuell erstellte Modelle oder Anwendungen mit anderen Systemen verarbeitet werden? Wie können sie veränderungsfrei übertragen werden?

6.2.3.2 Bereinigung der Edge-Komponente

Wie kann die Edge-Komponente bereinigt werden?

Die Edge-Komponente muss zum Abschluss bereinigt und die enthaltenen Daten müssen nicht wiederherstellbar gelöscht werden.

ID	Frage
EX1.1	Welche Daten sind in der Edge-Komponente enthalten? Gibt es versteckte Daten auf der Edge-Komponente? Backups? Telemetriedaten? Konfigurationsdaten, die Rückschlüsse auf Netzumgebungen zulassen?
EX1.3	Wie werden alle Daten unwiderrufbar gelöscht? Gibt es eine Funktion, die die Edge-Komponente oder den auf ihr genutzten Bereich in den Originalzustand versetzt?

7 Anhang 1 Literaturverzeichnis

[1] https://de.wikipedia.org/wiki/Content_Delivery_Network
[2] https://www.nist.gov/publications/fog-computing-conceptual-model
[3] https://www.iiconsortium.org/pdf/OpenFog_Reference_Architecture_2_09_17.pdf
[4] https://www.etsi.org/technologies/multi-access-edge-computing
[5] https://elijah.cs.cmu.edu/
[6] https://www.cloudflare.com/de-de/learning/cloud/ngfw-vs-fwaas/
[7] https://www.itwissen.info/next-generation-firewall-NGFW.html
[8] https://www.computerweekly.com/de/definition/Next-Generation-Firewall-NGFW
[9] C5 BSI
[10] Grundschutzkompendium BSI Baustein OPS2.2
[11] Technische Richtlinie des BSI zu SBOM
[12] Mindeststandard des BSI - Nutzung externer Cloud Dienste
[13] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen_node.html
[14] Verteilte Systeme - Prinzipien und Paradigmen von Andrew S. Tanenbaum und Maarten van Stehen

8 Anhang 2 Abbildungsverzeichnis

Abbildung 1: Zusammenspiel zwischen Cloud, Edge und Fog Computing
Abbildung 2: NIST-Modell Fog Computing [2]
Abbildung 3: Angepasstes Edge- und Fog-Modell für die BSI Arbeit
Abbildung 4: Modellhafter Aufbau eines Cloudlets im angepassten Modell für die BSI Arbeit
Abbildung 5: IoT-basierte Verkehrsregulierung
Abbildung 6: Umsetzung von Predictive Maintenance
Abbildung 7: Beispiel für Edge-Komponente beim Einsatz beim Hochfrequenzhandel bei der Börse
Abbildung 8: Lebenszyklus einer Edge-Komponente aus Sicht des Anwenders