Effiziente Cyber-Resilienz

KIT
Dr. Kaibin Bao
kaibin.bao@kit.edu

Dr. Ghada Elbez
ghada.elbez@kit.edu

Notwendigkeit von Cyber-Resilienz

Mit der Energiewende entwickelt sich das Energieversorgungsnetz von einer hierarchischen Infrastrukturarchitektur zu einem dezentralen, zellulären Energienetz. Dieser Wandel erhöht die Komplexität des gesamten Systems, bestehend aus Netz- und Anschlusspunkten sowie den zugehörigen Komponenten. Die zuvor geltenden statistischen Annahmen über den Energiefluss treffen nicht mehr zu. Das Netz muss nun flexibel und dynamisch auf veränderte Bedingungen reagieren können, beispielsweise auf Spannungsspitzen durch hohe Leistungsbereitstellung dezentraler erneuerbarer Energiequellen oder auf Engpässe, die entstehen, wenn Energie für das gleichzeitige Laden mehrerer Elektrofahrzeuge benötigt wird. Dies erfordert den Ausbau von anpassungsfähigen Netzkomponenten. Die damit einhergehende dynamische Beanspruchung macht eine digitale Überwachung der Betriebsmittel in der Primärtechnik notwendig. Die Sekundärtechnik wird durch Informations- und Kommunikationstechnologie (IKT)-Komponenten ergänzt, um Funktionen wie Fernüberwachung, Fernwartung und Fernsteuerung zu ermöglichen.
Diese Digitalisierung des Energienetzes stellt insbesondere auf der Verteilnetzebene aufgrund der großen Anzahl von Netzkomponenten und oft mangelnder Konnektivität eine Herausforderung dar. Gleichzeitig erhöht die Integration der Netzbetriebsmittel in ein IKT-Netzwerk die Angriffsfläche für Cyberangriffe, was besondere Aufmerksamkeit in Bezug auf Cyber-Sicherheit erfordert.

Zielstellung für Cyber-Resilienz

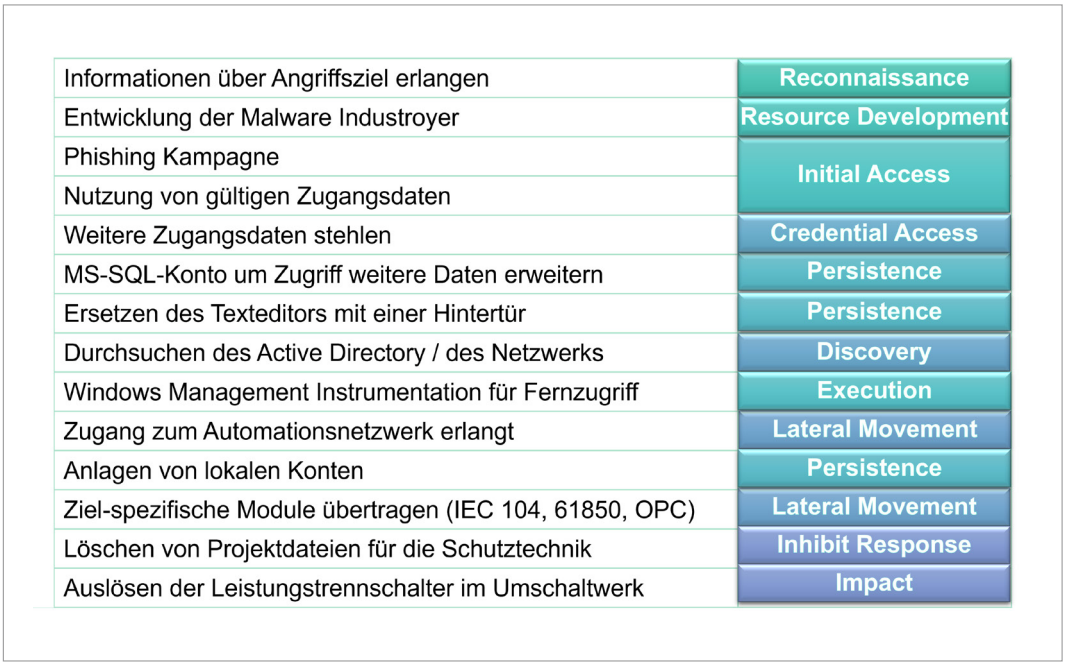
Laut NIST SP 800-160 (Sonderpublikation der U.S.-Behörde NIST, National Institute of Standards and Technology) bezeichnet die Cyber-Resilienz die Fähigkeit einer Organisation, den operativen Betrieb trotz Cyberbedrohungen aufrechtzuerhalten und sich von diesen Bedrohungen zu erholen [NIST SP 800-160]. Das Themenfeld ist eng verwandt mit der Cyber-Sicherheit, deren Hauptziel es ist, die Ausnutzung von Sicherheitslücken zu verhindern bzw. die Auswirkungen einer solchen Ausnutzung zu verringern.

Sowohl in der Cyber-Sicherheit als auch in der Cyber-Resilienz ist es wichtig, die Anforderungen und den Kontext des Systems genau zu spezifizieren: Vor welchen Akteuren soll das System geschützt werden und gegen welche Angriffe? Dies folgt dem Zitat von Bruce Schneier: „The first questions to ask are: ‚Secure from whom?' and ‚Secure against what?' […] Like any adjective, ‚secure' is meaningless out of context." [Schneier15].
Im Gegensatz zur Cyber-Sicherheit, die sich auf Prävention konzentriert, beschäftigt sich die Cyber-Resilienz mit der Frage, wie auf einen Sicherheitsvorfall reagiert wird. Angesichts der Tatsache, dass Sicherheitslücken auf absehbare Zeit nicht vollständig vermieden werden können, erweist sich die Cyber-Resilienz als das entscheidende Themenfeld, mit dem sich die Sicherheit von Organisationen konkret und wirksam stärken lässt.

Beispiel eines Cyber-Angriffs

Als illustratives Beispiel, wie ein gezielter Cyber-Angriff gegen ein Energiesystem ablaufen kann, wird im Folgenden skizziert, wie der Cyber-Angriff Ende 2016 gegen das ukrainische Stromnetz abgelaufen ist. Bei diesem Angriff wurden an fünf Umspannwerken im Gebiet Kyiv die Schutzeinrichtungen ausgelöst. Die Wiederherstellung benötigte etwa eine Stunde. Als Bedrohungsakteuer wurde die staatlich finanzierte Gruppe Sandworm identifiziert, die einen auf Energiesysteme spezialisierte Malware Industroyer, auch bekannt als CrashOverride verwendet hatte.
Zu Beginn des Ukraine-Kriegs 2022 wurde die Weiterentwicklung Industroyer2 gesichtet. Da zum Vorgehen im Jahr 2016 mehr bekannt ist, wird dieser Fall diskutiert.

Ein realer Cyber-Angriff erfolgt in mehreren Schritten. In der Sicherheitsbranche wird das MITRE ATT&CK-Framework verwendet, um diese Schritte zu klassifizieren [MITRE].



▶ *Abbildung 1*

Verlauf eines Cyberangriffs auf Energiesysteme

Das Beispiel zeigt den Angriff auf das ukrainische Energienetz 2016 mit Hilfe von Industroyer.

(rechte Spalte: Klassifizierung der einzelnen Schritte nach dem MITRE ATT&CK-Framework)

Die darin beschriebenen Taktiken werden im Folgenden verwendet, um die Angriffsschritte darzustellen (▶ Abbildung 1):

- Reconnaissance
  Der Angriff beginnt mit einer gründlichen Recherche des Angriffsziels. Es werden Informationen über Organisationsstrukturen, Lieferketten, Adressen, eingesetzte Hard- und Software ermittelt.
- Resource Development
  Um eine maßgeschneiderte Malware zu entwickeln, die effektiv in der spezifischen Umgebung des angegriffenen Unternehmens funktioniert, sind all diese Informationen von entscheidender Bedeutung. Im vorliegenden Fall wurden spezielle Module der Malware Industroyer entwickelt. Diese Module sind auf die weit verbreiteten Kommunikations- und Steuerungsprotokolle von Netzbetriebsmitteln sowohl im europäischen als auch im asiatischen Raum abgestimmt.
- Initial Access
  Wenn ausreichend Informationen vorhanden sind, etwa darüber, welche Person in welchem Kontext angeschrieben werden muss, um glaubwürdig zu wirken, kann die Phishing-Kampagne gestartet werden. Genau das ist im Januar 2016 passiert als durch eine Phishing-Kampagne die Daten der ersten Benutzerkonten ermittelt werden konnte, mit denen die Angreifer den ersten Fuß im Unternehmen hatten.
- Credential Access
  Durch den Zugriff auf die ersten Rechner konnten die Angreifer dann Software wie ScreenGraber und Keylogger zur Überwachung der Nutzereingaben installieren. Damit konnten sie weitere Konten erspähen, um mehr Zugriffsrechte zu erlangen und tiefer ins Netz einzudringen.
- Persistence
  Die Angreifer haben daraufhin herausgefunden, dass ein Datenbankserver auf MS-SQL-Basis betrieben wird. Dieser war mit weiteren Netzen verbunden, so dass man über diesen Hebel zwischen Januar und Dezember 2016 immer tiefer in die verschiedenen Unternehmensnetzwerke eindringen konnte.
  In einem weiteren Schritt wurde der Texteditor von Windows durch einen manipulierten Texteditor ersetzt, der eine integrierte „Hintertür" besaß, um noch einen zusätzlichen Zugriffsweg in das Unternehmen zu sichern, für den Fall, dass die bisher genutzten Zugriffswege in das Unternehmen entdeckt und versperrt werden sollte.
- Lateral Movement
  Der Prozess, bei dem Angreifer fortlaufend neue Computer und Netzwerke entdecken, die ihnen Zugang zu weiteren Systemen und Netzwerken gewähren, wird als "Lateral Movement" bezeichnet. Dieses schrittweise Vordringen durch ein Netzwerk mit dem Ziel, an Schlüsseldaten zu gelangen, wiederholt sich dabei mehrfach.
  In unserem Beispiel entdeckten die Angreifer im Dezember 2016 ein System, das Zugriff auf das Automationsnetz (Operational Technology, OT) des Energieversorgers hatte, so dass sie sich dort lokale Konten anlegen und den Zugriff sichern

konnten. Danach haben sie spezifische Module entwickelt, die gezielt auf die Automations- und Steuerprotokolle des Energiesystems fokussiert waren.

- Inhibit Response
  Um die Wiederherstellung nach dem Angriff zu erschweren, besaß die Malware zusätzliche Module mit der Funktion, die Projektdateien und die Konfiguration der Schutzgeräte zu löschen.
- Impact
  Die spezifisch für das Energiesystem entwickelten Module wurden in das Automationsnetz eingespeist. Mithilfe des Aufgabenplaners (Task Scheduler) lösten sie zu einem festgelegten Zeitpunkt zahlreiche Schutzgeräte aus, um eine Trennung von mehreren Stromnetzabschnitten zu erreichen. Dies führte am 17. Dezember 2016 zu einem Stromausfall, der ein Fünftel von Kiew betraf.

Tatsächlich gab es noch wesentlich mehr Zwischenschritte, aber schon die Aufzählung der Schlüsselereignisse zeigt, dass ein Angriff nicht über Nacht erfolgt ist. Es funktioniert nicht wie in Filmen, wo innerhalb weniger Stunden praktisch jedes Ziel erreicht werden kann. In der Realität nimmt ein Cyberangriff viel Zeit in Anspruch, erfordert zahlreiche Zwischenschritte und gründliche Vorbereitung. In unserem Beispiel dauerte es von Januar bis Dezember 2016 – also ein ganzes Jahr – vom ersten Eindringen bis zum eigentlichen Angriff. Während dieses Zeitraums bestehen fortwährend Möglichkeiten, das System zu überwachen und Angreifer gegebenenfalls zu identifizieren und zu isolieren.

Im Jahr 2022 fand ein weiterer Angriff auf die ukrainische Energiewirtschaft statt mit der Weiterentwicklung Industroyer2. Dieser Angriff war weniger erfolgreich, da schon die Phishing-Kampagnen schnell genug erkannt wurden und nur wenig Schaden bewirken konnten.

Wie konnte diesmal ein großflächiger Stromausfall verhindert werden? Cyber-Resilienz verhinderte nicht, dass überhaupt der erste Fuß ins Unternehmen gesetzt wurde. Sie sorgte aber für die Widerstandsfähigkeit der Organisation, trotz Angriffen und Sicherheitslücken den operativen Betrieb aufrecht zu erhalten. Und falls doch mehr passiert, sorgt Cyber-Resilienz dafür, dass sich das System von diesen Angriffen erholt und der ursprüngliche Zustand schneller wiederhergestellt werden kann.

Ziele von Cyber-Resilienz

Entsprechend dem Standard der U.S.-Behörde NIST (National Institute of Standards and Technology) gibt es für Cyber-Resilienz vier große Ziele (▶ Abbildung 2) [NIST SP 800-160]:

1. Bereitschaft
   Zunächst braucht es die informierte Bereitschaft gegenüber möglichen Cyberangriffen und den internen und externen Umständen, die zu einem Angriff führen können. Wo sind mögliche Sicherheitslücken im eigenen System? Wie agieren Hacker-Gruppen (Advanced Persistent Threat, APT), wie sehen deren aktuelle Taktiken aus? Dieses Wissen heißt „Cyber Threat Intelligence (CTI)“. Basierend auf diesem Wissen erhöhen Schulungen und die Implementierung von präventiven Maßnahmen die Widerstandsfähigkeit gegenüber Angriffen.
2. Widerstehen
   Als weiteres Ziel gilt es, Angriffen möglichst standzuhalten. Trotz Sicherheitsvorfällen sollen die wesentlichen Geschäftsfunktionen bzw. die Funktion der kritischen Infrastruktur aufrechterhalten werden („Business Continuity“).
3. Wiederherstellung
   Im Falle eines erfolgreichen Angriffs ist es entscheidend, umgehend zu identifizieren, welche Bereiche der Unternehmensinfrastruktur und der cyber-physikalischen Systeme betroffen sind. Anschließend muss der Angriff in diesen Bereichen isoliert werden, um eine weitere Ausbreitung zu verhindern. Für eine effektive Wiederherstellung ist es essenziell, genau zu verstehen, welche Systemkomponenten beeinträchtigt wurden.

▶ *Abbildung 2*

Ziele von Cyber-Resilienz

Dies ermöglicht es, gezielt nur die tatsächlich betroffenen Systeme wiederherzustellen, anstatt eine vollständige Ersetzung aller Unternehmenssysteme vornehmen zu müssen. Diese zielgerichtete Herangehensweise minimiert die Ausfallzeit und stellt die betrieblichen Funktionen schneller wieder her, ohne unnötige Ressourcen zu beanspruchen.

4. Anpassung
   Als letztes Ziel gilt es, aus realen oder simulierten Angriffen zu lernen. Managementstrukturen und IT-Systeme werden angepasst, um künftigen Angriffen besser zu widerstehen bzw. um das System nach einem Angriff schneller und effizienter wiederherstellen zu können.

Cyber-Resilienz in der Gesetzgebung

Cyber-Resilienz ist nicht nur ein technisches Ziel, sondern auch ein gesetzliches Erfordernis. Jüngst mussten sich die Energieversorger und Energienetzbetreiber in Deutschland mit dem IT-Sicherheitsgesetz 2.0 [BSI IT-SIG 2.0] auseinandersetzen, weil im Mai 2023 die Übergangsfrist endete, um Systeme zur Angriffserkennung (SzA) zu implementieren. Das IT-Sicherheitsgesetz 2.0 ist ein Änderungsgesetz, dass das BSI-Sicherheitsgesetz und die BSI-KritisVerordnung [BSI KritisV] betrifft und letztendlich die EU-Sicherheitsrichtlinie NIS 1 (Network und Information Security) [EU NIS] umsetzt.
Die EU-Sicherheitsrichtlinie NIS 2 [EU NIS2] zur Stärkung der Cyber-Sicherheit wurde Ende 2022 beschlossen und muss bis Oktober 2024 in nationales Recht umgesetzt werden, woran schon gearbeitet wird.

Eine weitere wichtige Initiative ist die EU-Richtlinie zur Resilienz kritischer Einrichtungen [EU RCE], die zusätzliche Anforderungen stellt.
Diese Gesetze und Richtlinien verpflichten Betreiber kritischer Infrastrukturen und größere, systemrelevante Unternehmen, ihre Anstrengungen zur Gewährleistung der Cyber-Resilienz zu verstärken. Die Webseite www.openkritis.de bietet einen umfassenden Überblick über die geltenden Vorschriften.
Die Gesetzgebung fordert also Mindeststandards in technischen und organisatorischen Bereichen, um die Ziele der Cyber-Resilienz zu erreichen. Dazu gehört eine verpflichtende Risikobewertung, die Unternehmen durchführen müssen, um potenziell gefährdete Bereiche zu identifizieren. Zudem ist eine zentrale Sicherheitsüberwachung erforderlich, um Angriffe frühzeitig zu erkennen und Schäden zu verhindern.

Für deutsche Unternehmen sind auch internationale Normen relevant, die einige Bausteine beschreiben, wie Cyber-Resilienz gestärkt werden kann:

- Die ISO 27000-Familie beschreibt ein Management-system für Informationssicherheit (ISMS) und wie dieses dann auch zertifiziert werden kann.
- Speziell für das Energiesystem ist IEC 62443 mit Fokus auf Automationssysteme relevant. IEC 62351 adressiert die Cyber-Sicherheit für digitale Komponenten in Energiesystemen.
- In der ISO 22301 werden Anforderungen an Management-Systeme für betriebliche Kontinuität beschrieben.

Bausteine für Cyber-Resilienz

Einige Beispiele für technische und organisatorische Maßnahmen zur Steigerung der Cyber-Resilienz sind:

- Die gesetzlich geforderten Systeme zur Angriffserkennung beziehen sich wahrscheinlich auf Lösungen für Security Information and Event Management (SIEM) oder Extended Detection and Response (XDR) in Kombination mit einem Angriffserkennungssystem (Intrusion Detection System, IDS).
  Trotz unterschiedlicher Bezeichnungen ist das Grundprinzip solcher Systeme ist vergleichbar und wird in nächsten Abschnitt unter dem Begriff Sicherheitsüberwachung ausführlicher beschrieben.
- Netzwerksegmentierung ist ein Prinzip für die Architektur der Netzwerkinfrastruktur. Sie beschreibt die Trennung des Netzwerks in möglichst kleine, fachlich zusammenhängende Teile. Dies schränkt die Bewegungsfreiheit eines potenziellen Angreifers ein. Mindestens das cyberphysikalische System sollte von dem betriebswirtschaftlichen Unternehmensnetzwerk getrennt sein.
  Netzwerksegmentierung lässt sich durch „Zero Trust“ ergänzen: Die Kommunikation zwischen Netzwerkteilnehmern muss stehts verifiziert werden. Selbst wenn die Teilnehmer im selben Netzwerksegment sind, gibt es kein implizites Vertrauen.
- Notfallpläne sind wichtig, um im Falle eines Angriffs vorab festgelegte Reaktionen effektiv umsetzen und die Systeme wiederherstellen zu können.
- Prävention betrifft mehrere Aspekte, das Unternehmen gegenüber Angriffen zu härten: Beispielsweise Risikomanagement unter Berücksichtigung aktueller Cyber Threat Intelligence, Mitarbeitendenschulungen und Bewusstseins-

bildung gegenüber auf menschliche Faktoren zielende Angriffsschritte, feingranulare Zugriffskontrolle, Management von Schwachstellen, Asset- und Patchmanagement, und Antiviren- und Malware-Schutz.
- Für die eigentliche Wiederherstellung nach einem Angriff ist ein effektives Backup- und Wiederherstellungskonzept notwendig.

Sicherheitsüberwachungssysteme

Sicherheitsüberwachungssysteme funktionieren vereinfacht wie in ▶ Abbildung 3 dargestellt: Die IT/OT-Infrastruktur eines Unternehmens besteht aus Endpunkten und Netzwerken (linke Seite der Abbildung). Endpunkte sind PCs, Server, mobile Geräte, sowie Automation- und Steuersysteme.
Zum Zweck der Angriffsüberwachung wird das hier vereinfacht dargestellt. In der Realität sollten sich die Geräte nicht in getrennten Netzwerken befinden.

Um Angriffe aufzudecken, werden Informationen über Benutzer- und Systemaktivitäten sowie System- und Anwendungsereignisse von Endpunkten gesammelt. Auf der anderen Seite wird der Netzwerkverkehr überwacht. Während die Daten von einem Endpunkt feingranulare Informationen über die Systemaktivität liefern, enthalten Netzwerkdaten auch Informationen von Geräten, bei denen keine Endpunktüberwachung installiert werden kann.

Alle Informationen werden zentral in einem Überwachungssystem gesammelt und in ein einheitliches Format langfristig in einer Datenbank gespeichert. Auffälliges Verhalten wird automatisiert über ein Alarmsystem gemeldet. Diese Meldungen bearbeiten dann Mitarbeitende vom Security Operating Center (SOC), indem sie sie mit anderen Ereignissen in Bezug gesetzt und bewertet werden können. Wird zu einem späteren Zeitpunkt bekannt, wie neuartige Angriffe stattfinden, kann nach diesen Mustern nachträglich in der Ereignisdatenbank gesucht werden.
Diese Abläufe sind sehr personalintensiv. An dieser Stelle kann die Forschung mithelfen, die Prozesse effizienter zu gestalten.

Herausforderungen bei der Umsetzung von Sicherheitsüberwachungssystemen

Automatisierung der Angriffserkennung

Bei Automatisierungen stellt sich die prinzipiell die Frage, welches Ausmaß zielführend ist. Denn je stärker die Automatisierung, umso wahrscheinlicher wird es auch, dass man reale, neuartige Angriffe übersehen werden.

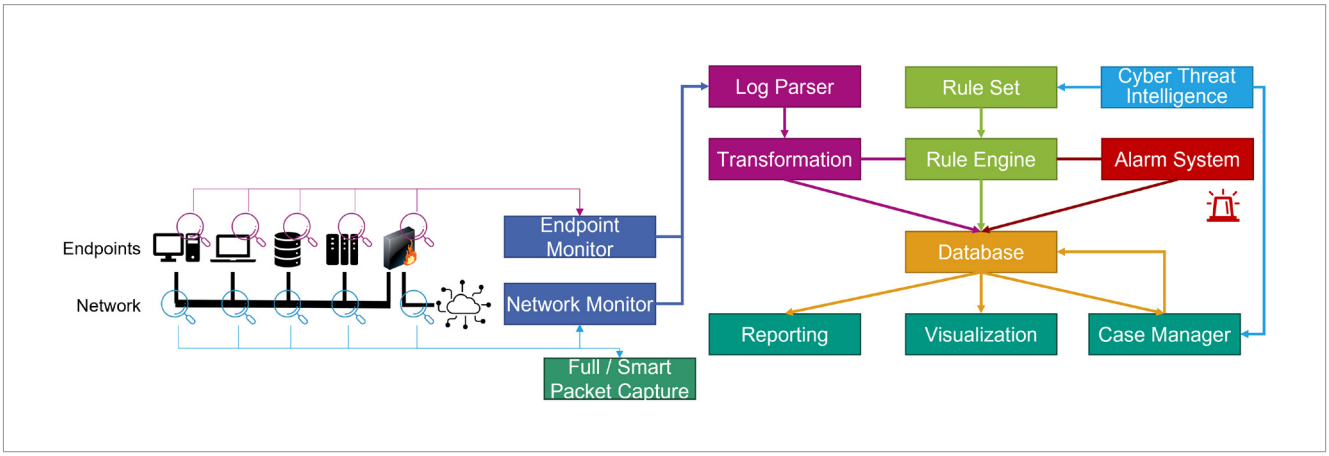
Sichtbarkeit

Das Sammeln der Informationen aus allen Netzsegmenten und Endpunkten in der gesamten Infrastruktur ist aufwendig. Werden Teile nicht in die Sicherheitsüberwachung integriert, besteht die Gefahr, dass Angriffsschritte nicht erkannt oder nachvollzogen werden können.

Überwachungsintensität / Bandbreite / Performance

Bei der Implementierung eines Überwachungssystems ist eine Abwägung zu treffen, wie feingranular System- und Netzwerkaktivität aufgezeichnet werden soll. Eine feingranulare Aufzeichnung ermöglicht eine Aufzeichnung von unbekannten Angriffsmustern, erfordert allerdings mehr Speicherplatz und geht ggf. mit Performanceeinbußen auf den überwachten Systemen einher.

Der Einsatz von Überwachung in einem geografisch verteilten System stellt zudem höhere Anforderungen an die Kommunikationsbandbreite.



▶ *Abbildung 1*

Sicherheitsüberwachungssystem

(Quelle: eigene Grafik basierend auf Seminararbeit über Sicherheitsüberwachungssysteme (Quelle: [RR23])

In der Realität ist die Sichtbarkeit kein größeres Problem, doch nicht jeder Punkt im Energienetz ist kommunikationstechnisch gut erreichbar. Aktuell stehen die Übertragungsnetzbetreiber diesbezüglich gut da, weil sie schon jetzt viel Kommunikationstechnologie einsetzen. Aber bei den Verteilnetzbetreibern ist problematisch, dass vieles noch nicht digitalisiert oder zumindest kommunikationstechnisch angebunden ist.

Security by Design

Schon in der Entwurfsphase sollte das System darauf optimiert werden, dass ein Angreifer es möglichst schwer hat, indem Angriffswege versperrt werden.

Adaption auf Zielsysteme erforderlich

Sicherheitslösungen müssen stehts aufwendig konfiguriert werden, um zunächst alle Informationsquellen verarbeiten zu können und schließlich zwischen normales Verhalten und potenziellen Angriffen unterscheiden zu können.

Faktor Mensch

Die rechtmäßigen Nutzer der IT-Infrastruktur sind potenziell gegenüber Social Engineering verwundbar und halten für eine durch technische Mittel kaum zu stopfende Sicherheitslücke in einem Unternehmen offen. Zudem ist menschliches Verhalten schwer zu modellieren und beeinträchtigt eine Unterscheidung zwischen Angriff und normales Verhalten.

Forschungsprojekte

Die folgenden Forschungsprojekte entwickeln einige Bausteine, um Cyber-Resilienz zu unterstützen:

Security Lab Energy im Energy Lab 2.0 (KIT)

Diese Forschungsanlage dient der Emulation von Cyber-Angriffen auf Energiesystemen und der Erforschung von neuen Erkennungsansätzen. Zunächst wird ein repräsentatives Energiesystem nachgeahmt. Die Physik für Wechselstrom, Spannungen und Ströme wird simuliert. Die Steuergeräte (Operational Technology) für Generatoren, Transformatoren und Schutzgeräte existieren real und sind an die Physiksimulation angebunden. Ein weiterer Bestandteil der Forschungsanlage ist die virtuelle Unternehmens-IT-Infrastruktur. Somit können komplexe Cyberangriffe wie das einführende Beispiel vollständig emuliert (nachgeahmt) werden. Mit der simulierten Physik haben Angriffe keine dauerhaften Konsequenzen und sind beliebig reproduzierbar.

KASTEL Security Lab Energy

Das KASTEL Security Lab Energy enthält zunächst einen vergleichbaren Aufbau wie das oben beschriebene Security Lab Energy. Zusätzlich existiert eine weitere Forschungsanlage, die eine Umspannstation nachbildet mit Komponenten unterschiedlicher Hersteller. Ein dritter Forschungsaufbau fokussiert sich auf die Kommunikation über Software Defined Networking (SDN).
Zielsetzung ist ebenfalls die Nachahmung von komplexen Cyberangriffen auf Energiesysteme in einem realitätsnahen Umfeld.

Angriffserkennung basierend auf Ereignisprovenienz

Bei diesem Forschungsprojekt geht es um eine bessere Nachverfolgbarkeit, wie einzelne Schritte in einem Cyberangriff tatsächlich stattfinden. Da einzelne Systemereignisse nur begrenzte Aussagekraft über die Angriffsmethoden haben, werden die Systemereignisse aufgezeichnet und in einem „Provenienz-Graph“ miteinander in Bezug gesetzt. So sind Rückschlüsse auf die Angriffsschritte möglich und die vollständige Angriffskette kann basierend darauf automatisiert rekonstruiert werden.

Anomalie-basierte Angriffserkennung

Mit der automatisierten, Anomalie-basierten Angriffserkennung ist man in der Lage, unbekannte und neuartige Angriffe zu erkennen. In der Arbeit von Dr. Elbez [Elbez23] wurden unterschiedliche Angriffe betrachtet, die zu verfälschten Meldungen zwischen Schutzsystemen in einem Umspannwerk führten. Mit einem autoregressiven Modell konnten solche Angriffe mit einer hohen Trefferquote erkannt werden.

Forschungsbedarf

Es gibt mehrere Punkte, für die Forschungsbedarf besteht.Unterschiedliche Forschungslabore für Cyber-angriffsemulationen sind wünschenswert, um Angriffserkennungsansätze in unterschiedlichen Umgebungen prüfen zu können.
Leider besteht immer noch eine große Lücke zwischen Wissenschaft und Praxis, da es für die Forschung sehr aufwendig ist, die Komplexität realer Angriffe nachzubilden. Dementsprechend ist die Qualität von wissenschaftlichen Datensätzen beschränkt. Daten von realen Angriffen in Firmen sind nicht öffentlich verfügbar.
Für Cyber-Resilienz ist es auch wichtig, dass verschiedene Forschungsdisziplinen zusammenarbeiten. Konkret in unserem Forschungsfeld mangelt es Informatiker*innen an Wissen über Energiesysteme und umgekehrt haben Elektrotechniker*innen begrenztes Wissen über IT und Cyberangriffe.

Zusammenfassung

Energiewende und Digitalisierung erfordern zwingend Cyber-Resilienz, damit das Energiesystem auch künftig zuverlässig funktionieren kann. Cyber-Resilienz beschäftigt sich mit dem Umgang mit unvermeidlichen Angriffen und wie einUnternehmen sich davon möglichst schnell erholen kann, um seinen Betrieb effizient wiederaufzunehmen.
Dabei ist zu berücksichtigen, dass das gesamte cyberphysikalische System aus technischen, organisatorischen und menschlichen Elementen besteht.
Forschung kann durch die Nachbildung von repräsentativen cyberphysikalischen Systemen und durch die Nachbildung von komplexen Cyberangriffen Lösungen für die Ertüchtigung von Cyber-Resilienz finden. Für diese Aufgabe braucht es interdisziplinäre Forschung.

Referenzen

Veröffentlichungen und Internet-Quellen

- [Schneier15] Schneier, Bruce. (2015). Secrets and lies: digital security in a networked world. John Wiley & Sons.
- [Elbez23] Elbez, Ghada, Klara Nahrstedt, and Veit Hagenmeyer. "Early Attack Detection for Securing GOOSE Network Traffic. " IEEE Transactions on mart Grid (2023). https://doi.org/10.1109/TSG.2023.3272749
- [GM23] Google, & Mandiant. (2023). Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape. https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
- [EX22] Exabeam. SIEM Architecture: Technology, Process and Data. https://www.exabeam.com/explainers/siem/siem-architecture/. abgerufen am 2022-05-23
- [RR23] Richard Rudolph. Cyber Incident Detection and Response. Februar 2023.
- [MITRE] MITRE ATT&CK Framework. https://attack.mitre.org. abgerufen am 2022-05-23
Gesetze, Richtlinien und Verordnungen
- [BSI KritisV] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung-BSI-KritisV) https://www.gesetze-im-internet.de/bsi-kritisv/index.html
- [BSI IT-SIG 2.0] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf
- [EU NIS] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz-und Informationssystemen in der Union https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016L1148
- [EU NIS2] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14.Dezember 2022 über Maßnahmen für ein hohesgemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr.910/2014 und der Richtlinie (EU)2018/1972 sowie zur Aufhebung der Richtlinie (EU)2016/1148 (NIS-2-Richtlinie) (Text von Bedeutung für den EWR) https://eur-lex.europa.eu/eli/dir/2022/2555
- [EU RCE] Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14.Dezember 2022 über die Resilienz kritischerEinrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (Text von Bedeutung für den EWR) https://eur-lex.europa.eu/eli/dir/2022/2557/oj

Normen

- [NIST SP 800-160] National Institute of Standards and Technology (2021), Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, NIST Special Publication 800-160, Volume 2, Revision 1, https://doi.org/10.6028/NIST.SP.800-160v2r1
- [ISO 27001] ISO/IEC 27001: Information s ecurity management systems. International Organization for Standardization, Geneva, Switzerland. https://www.iso.org/standard/27001
- [IEC 62443] IEC 62443: Industrial communication networks - Network and system security. International Electrotechnical Commission, Geneva, Switzerland. https://webstore.iec.ch/searchform&q=IEC%2062443
- [IEC 62351] IEC 62351: Power systems management and associated information exchange - Data and communications security. International Electrotechnical Commission, Geneva, Switzerland. https://webstore.iec.ch/publication/6912
- [ISO 22301] ISO/IEC 22391: Security and resilience — Business continuity management systems. International Organization for Standardization, Geneva, Switzerland. https://www.iso.org/standard/75106.html