swisscom

Cybersecurity Threat Radar 2026

Geopolitik und disruptive Technologie als Bedrohungstreiber

Inhalt

«Vertrauen ist kein Versprechen, das man einmal abgibt, es ist eine Verantwortung, der wir uns jeden Tag neu stellen müssen. Als Innovators of Trust schützen wir nicht nur Daten, sondern die digitale Zuverlässigkeit und Souveränität der Schweiz.

Cybersecurity Threat Radar

Geopolitik und disruptive Technologie als Bedrohungstreiber

Jeden Tag schützen wir bei Swisscom nicht nur Systeme, sondern fördern auch die Digitalisierung der Schweiz. Millionen Menschen verlassen sich auf stabile Netze, sichere Kommunikation und digitale Resilienz. Als CSO sehe ich täglich, wie sich geopolitische Spannungen und technologische Sprünge direkt auf die Sicherheit auswirken. Bedrohungen entstehen heute global, ihre Auswirkungen können uns aber jederzeit auch lokal treffen.

Der hier vorliegende Cybersecurity Threat Radar ist unser Frühwarninstrument. Er zeigt uns, wohin sich Bedrohungen verschieben, welche Muster neu entstehen und wo Handlungsbedarf besteht. Besonders beschäftigt hat mich in diesem Jahr, dass wir erstmals Hybrid Warfare, die Vermischung klassischer militärischer Mittel mit Cyberangriffen, Desinformation und digitaler sowie politischer Einflussnahme, als neuen Bedrohungsvektor aufnehmen mussten. Diese Entwicklung macht deutlich, wie eng physische und digitale Sicherheit mittlerweile verknüpft sind.

Geopolitische Unsicherheiten und wirtschaftliche Interessenkonflikte führen zu einem Anstieg staatlich motivierter Cyberangriffe. Attacken, die nicht nur Unternehmen, sondern die digitale Stabilität der ganzen Schweiz herausfordern. Als Telekommunikationsanbieterin spüren wir, wie zentral Anpassungsfähigkeit und Resilienz geworden sind.

Auch disruptive Technologien verändern das Spielfeld. Künstliche Intelligenz, Quantencomputing und vernetzte Geräte eröffnen enorme Chancen für Innovation – und zugleich neue Angriffsflächen. Der Schutz der digitalen Schweiz und der Menschen, die täglich auf uns zählen, bleibt für Swisscom oberste Priorität.

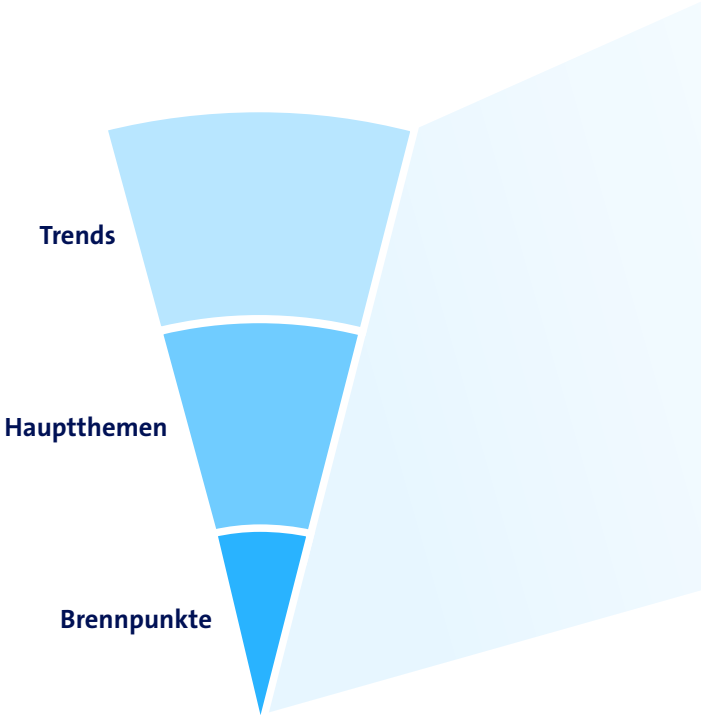
All das zeigt: Sicherheit ist keine Selbstverständlichkeit, sondern ein fortlaufender Prozess. Er verlangt vorausschauendes Handeln, die kontinuierliche Analyse neuer Bedrohungen und eine Sicherheitskultur, die im ganzen Unternehmen gelebt wird. Nur wenn wir unsere Schutzmassnahmen ständig weiterentwickeln und konsequent umsetzen, können wir den komplexen Risiken unserer Zeit effektiv begegnen und die digitale Schweiz zuverlässig stärken.

Marco Wyrsch
Head of Group Security
& Chief Security Officer

Lagebild – Bedrohungsradar

Im richtigen Moment auf Sicherheitsstrategien und -prozedere zurückgreifen zu können, die gefestigt und erprobt sind, hilft uns, mit Unvorhersehbarkeiten – sogenannten Schwarzen Schwänen – zurechtzukommen. Mit einer konsequenten Sicherheitskultur, Fehlertransparenz und gut ausgebildeten Mitarbeitenden schaffen wir die Grundlage für eine organisationale Resilienz.

Dafür müssen potenzielle Bedrohungen frühzeitig erkannt und systematisch erfasst werden. Um die Bedrohungslage und ihre Evolution abzubilden, verwenden wir den bekannten Cybersecurity Threat Radar.




Environment/Social
Dominant Players
Technology Dynamics
Organisation
Physical
Security Job Market
Geopolitical Situation / State Level Attacks
Data-Centric Risks
Identity Theft & Impersonation
Disinformation & Destabilisation
Political Influence
Hybrid Warfare
Environmental Influence
Targeted Sabotage
Unsecure IoT/OT
Digital Transformation Risks
UAS Threats
Energy Instability
Manipulated Generative AI
Cloud Ecosystem Dependencies
Legacy Protocols
Infrastructure Integrity
Subscriber Compromise
Agentic AI
Increased Complexity
DDoS Attacks
Ransomware
AI-Based Attacks
Supply Chain Attacks
Targeted Attacks
Unsecure AI
Residential Proxies
Fraud
Security Skills
Insider Threat
Quantum Computing
Infrastructure Misconfiguration
Fragile Workforce
Decentralised Development & Operations
Workplace Heterogeneity
● Herausforderungen
Today ● • • • ► Tendency

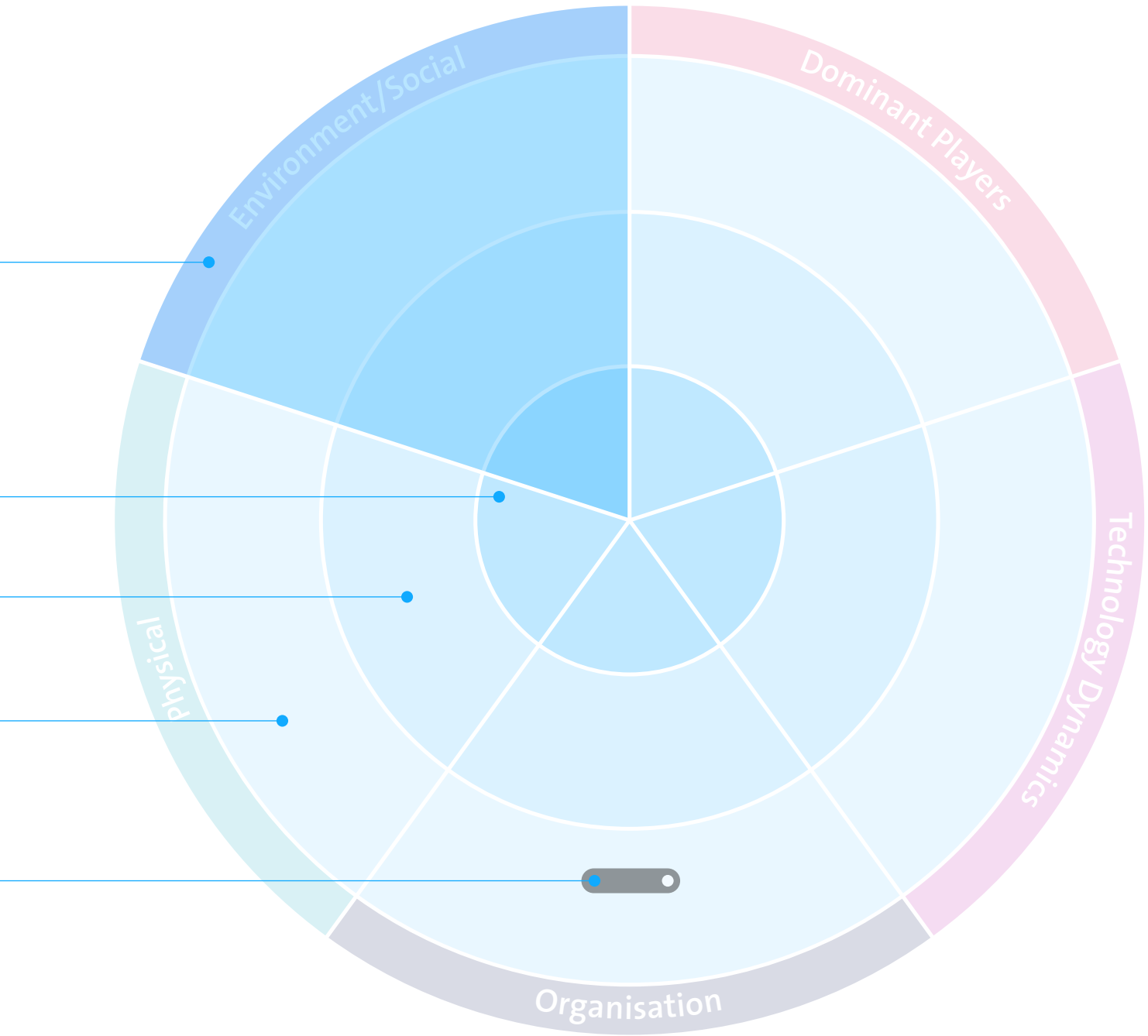
Methodik

Der Bedrohungsradar ist in fünf **Segmente** unterteilt, welche die unterschiedlichen Domänen der Bedrohungen voneinander abgrenzen. In jedem **Segment** können die dazugehörenden Bedrohungen einem von drei konzentrischen Kreisen zugeordnet werden. Die Kreise zeigen die Aktualität der jeweiligen Bedrohung an und damit auch die Unschärfe, die in der Beurteilung der Bedrohung liegt. Je näher die Bedrohung zum Kreismittelpunkt verortet ist, desto konkreter ist sie und umso wichtiger sind angemessene Gegenmassnahmen.

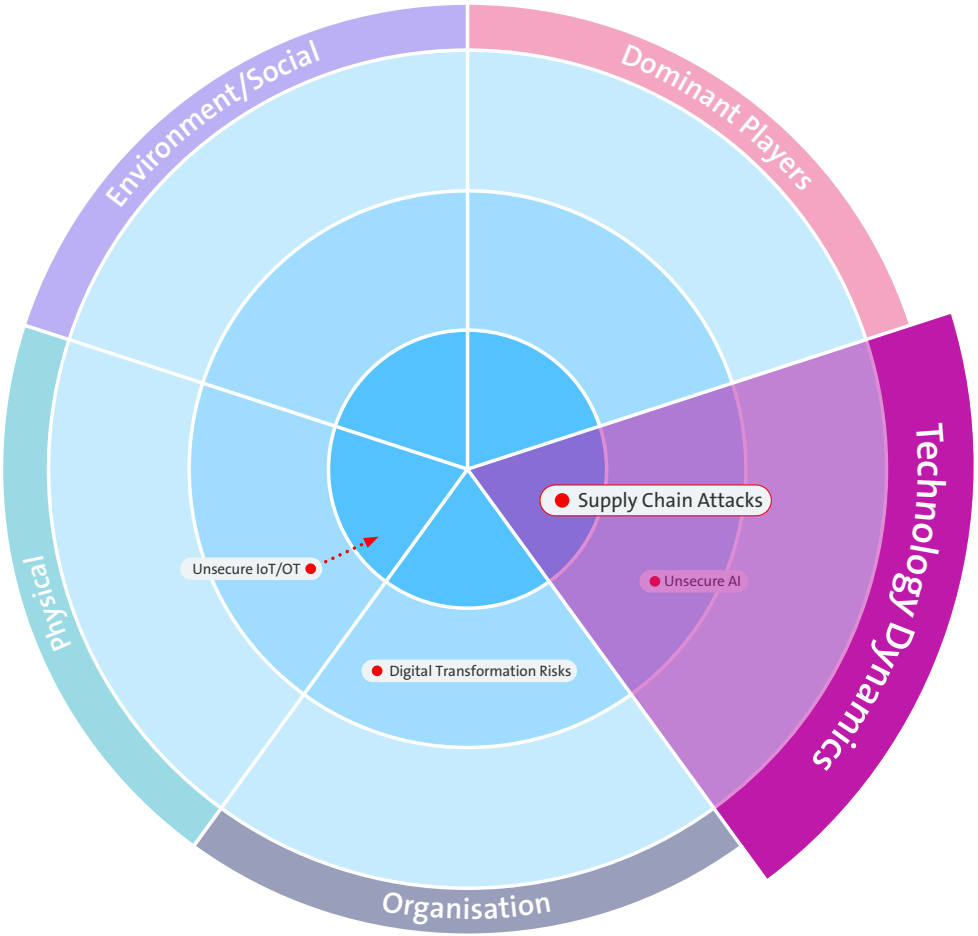
Die Kreise kennzeichnen wir als:

- **Brennpunkte** für Bedrohungen, die bereits real sind und mit relativ grossem Einsatz von Ressourcen bewältigt werden.
- **Hauptthemen** für Bedrohungen, die bereits vereinzelt eingetreten sind und mit einem normalen Ressourceneinsatz bewältigt werden. Oft bestehen geregelte Prozesse, um derartigen Bedrohungen effizient zu begegnen.
- **Trends:** Früherkennung für Bedrohungen, die noch nicht eingetreten sind oder aktuell nur sehr gering sind. Es wurden Projekte gestartet, um der zukünftig wachsenden Bedeutung dieser Bedrohungen frühzeitig begegnen zu können.

Weiter weisen die einzelnen, durch benannte Punkte gekennzeichneten **Bedrohungen** eine **Tendenz** auf. Diese kann in ihrer Kritikalität zunehmend, rückläufig oder stabil sein. Die Länge des Tendenzstrahls zeigt die erwartete Schnelligkeit auf, mit der sich die Kritikalität der Bedrohung ändern wird.


Environment/Social
Dominant Players
Technology Dynamics
Organisation
Physical

Die Software-Lieferkette in der Supply Chain: ein Karten-haus aus fremdem Code



In einer zunehmend digitalisierten Geschäftswelt sind Unternehmen auf eine Vielzahl von Softwarelösungen und -diensten angewiesen. Die Einbindung externer Komponenten und Module ist längst zum Standard geworden – und genau darin liegt eine der grössten Herausforderungen der heutigen IT-Sicherheit: Supply Chain Attacks, also Angriffe auf die Lieferkette von Software. Ein schwacher Baustein genügt, um das gesamte Kartenhaus zum Einsturz zu bringen.

Moderne Software entsteht aus hunderten externen Komponenten und automatisierten Build Pipelines. Herkunft und Qualität dieses Fremdcodes sind dabei oft nicht transparent nachvollziehbar, was die Identifikation von Schwachstellen erheblich erschwert. Genau diese Intransparenz macht die Software-Lieferkette zu einem bevorzugten Ziel für Angreifer: Bereits eine kompromittierte Bibliothek oder ein manipuliertes CI/CD-System kann sich auf tausende Unternehmen auswirken.

Besonders heikel ist, dass sich viele Unternehmen auf Komponenten verlassen, deren Sicherheitsniveau sie nicht selbst überprüfen können.

Aktuelle Bedrohungslage: Beispiele und Entwicklungstrends

Im Jahr 2025 machten Vorfälle im npm-Ökosystem (npm ist die grösste Registry für JavaScript-Pakete) wie «Shai-Hulud» deutlich, dass eine neue Realität eingetreten ist: Angreifer nehmen Open-Source-Code gezielt ins Visier und missbrauchen die Vertrauenskette populärer Pakete, um Malware über scheinbar legitime Updates zu verbreiten. Da Updates häufig ohne zusätzliche Sicherheitsprüfungen oder manuelle Kontrolle übernommen und dann als Abhängigkeiten weiterverbreitet werden, können sich solche Angriffe entlang der gesamten Software-Lieferkette besonders schnell ausbreiten.

Zudem bestehen sogenannte Single Points of Failure, zentrale Dienste oder Anbieter, deren Ausfall oder Kompromittierung, wie jüngst bei CrowdStrike, Microsoft oder Cloudflare, erhebliche Folgen für zahlreiche Unternehmen nach sich ziehen können.

Datenverlust, Betriebsunterbruch und Reputationsschäden

Die Folgen erfolgreicher Angriffe auf die Software-Lieferkette sind gravierend: Neben dem Verlust sensibler Daten drohen Betriebsunterbrüche, die im schlimmsten Fall zum Stillstand geschäftskritischer Prozesse führen können. Nicht zu unterschätzen sind zudem die Reputationsschäden, die durch öffentlich bekanntgewordene Sicherheitsvorfälle entstehen und das Vertrauen von Kund*innen, Partnern und Investoren nachhaltig erschüttern können.

Überprüfbarkeit und Resilienz stärken
Um den Herausforderungen der modernen Software-Lieferkette zu begegnen, sind technische und organisatorische Massnahmen gefragt. Dazu zählen unter anderem:

- Konsequente Dokumentation und Nachverfolgung aller eingesetzten Module und deren Aktualisierungen
- Regelmässige Sicherheitsüberprüfungen (Audits) und Penetrationstests entlang der gesamten Lieferkette
- Etablierung von klaren Prozessen zur Auswahl, Bewertung und Freigabe externer Software-Komponenten
- Einsatz von Monitoring-Lösungen, die verdächtige Aktivitäten frühzeitig erkennen und melden
- Entwicklung und Umsetzung von Update-Strategien, um bekannte Schwachstellen zeitnah zu schliessen

Regulatorisch markieren der **Cyber Resilience Act (CRA)** und die **Network and Information Security Directive 2 (NIS2)** der Europäischen Union einen Wendepunkt: Hersteller müssen nachweisen, wie ihre Software entstanden ist, Betreiber müssen diese Nachweise prüfen. SBOM (Software Bill of Materials), reproduzierbare Builds, Signaturen und dokumentiertes Schwachstellenmanagement werden somit verpflichtend. Integrität und Herkunft werden nicht mehr vorausgesetzt, sondern technisch nachgewiesen.

Zentral sind dabei zwei Konzepte:

- **Integrität:** Ist ein Update echt und unverändert?
- **Provenance:** Wie, wo und womit wurde es gebaut?

Standards wie SLSA (Supply-Chain Levels for Software Artifacts) oder signierte SBOM liefern erstmals fälschungssichere Nachweise.

> «Erst wenn jedes Software-Artefakt kryptografisch signiert und seine Herkunft zweifelsfrei belegbar ist, ist die Basis für echtes Vertrauen geschaffen.

Florian Lukavsky
Chief Innovation Officer, SignPath

Da solche Prüfungen manuell kaum möglich sind, übernehmen spezialisierte Plattformen für Software Supply Chain Security automatisierte, kryptografisch abgesicherte Attestierungen direkt im Build-Prozess. So wird Sicherheit überprüfbar und ist nicht mehr reine Vertrauenssache.

Auch organisatorisch ist ein Umdenken gefragt. Unternehmen müssen ihre Lieferkette kontinuierlich überwachen, Schwachstellen aktiv managen und ihre Partner zu Mindeststandards verpflichten, um resilient gegen Supply-Chain-Angriffe zu bleiben. Die Sensibilisierung der eigenen Mitarbeitenden für die Risiken und das Schaffen einer Sicherheitskultur sind ebenso zentrale Bausteine.

Resilienz und kontinuierliche Überprüfung als Schlüssel

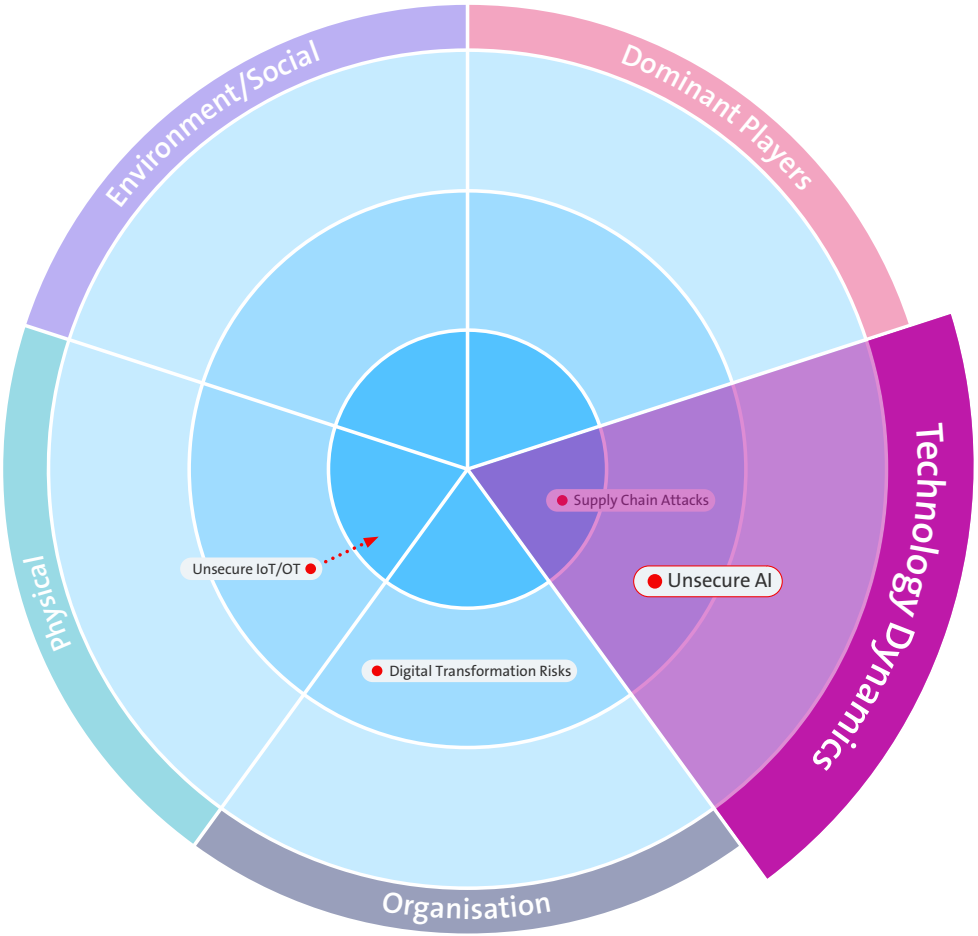
Die Bedrohung durch Supply Chain Attacks wird Unternehmen auch in Zukunft begleiten und weiter an Bedeutung gewinnen. Wer auf die Vorteile moderner, modularer Software setzt, muss sich der Risiken bewusst sein und konsequent in die eigene Resilienz investieren. Kontinuierliche Überprüfung, Transparenz und ein ganzheitliches Risikomanagement sind die Grundpfeiler, um das eigene IT-Kartenhaus auch in stürmischen Zeiten stabil zu halten und das «russische Roulette» in der Software-Lieferkette zu vermeiden.

> «Ganz ohne Vertrauen geht es heute noch nicht. Doch man sollte sich zwingend mit möglichen Schwachstellen in der Software-Lieferkette auseinandersetzen, etwa durch eine gezielte Bedrohungsmodellierung der gesamten Supply Chain.

Simon Röthlisberger
Security Architect

Herausforderungen und Trends

KI extrem: der Risiko-Multiplikator



Künstliche Intelligenz hat sich in beeindruckender Geschwindigkeit in vielen Bereichen unserer Gesellschaft und Wirtschaft ausgebreitet. Der Hype um KI-Technologien ist so gross, dass kritische Fragen rund um Sicherheit, Transparenz und Nachhaltigkeit in den Hintergrund treten können. Insbesondere der Bedrohungsvektor «Unsecure AI» zeigt, wie rasch Unwissenheit zu einer gefährlichen Systemarchitektur werden kann – mit Auswirkungen, die weit über die IT hinausreichen.

Dieser Artikel geht der Frage nach, warum wir uns mit ungesicherter KI auseinandersetzen müssen, wie diese Risiken entstehen und was Akteur*innen konkret tun können, um den Herausforderungen positiv und verantwortungsvoll zu begegnen.

Warum Unsecure AI zum Risiko wird

Die Begeisterung für KI verleitet oftmals dazu, Innovationen ohne fundiertes Verständnis oder ausreichende Sicherheitsüberlegungen einzuführen. KI-Systeme werden ohne Einschränkung eingesetzt, ohne zu wissen, wo und wie sie operative Entscheidungen beeinflussen, mit welchen Daten sie trainiert wurden oder wer im Entwicklungsprozess involviert war. Nicht selten werden Low-Code- und No-Code-Lösungen genutzt, deren Herkunft und Architektur für Anwender*innen nicht nachvollziehbar sind. Besonders kritisch ist, dass auch Partnerunternehmen KI integrieren, wodurch Supply Chain Risks (siehe Seite 10) entstehen, die schwer zu kontrollieren sind. Hinzu kommt, dass Schadsoftware immer häufiger direkt beim Coding – etwa durch generative KI – in Systeme eingeschleust wird.

Gefahr droht aber nicht nur durch Technik. Fehlendes Know-how auf Seiten der Nutzer*innen und der Cyber-Expert*innen verschärft das Problem. Der Trugschluss, dass Junior-Fachkräfte durch KI ersetzt werden könnten, führt zu einer Kompetenzlücke, die mittelfristig die gesamte Security-Struktur, inkl. Bereiche wie Data Quality Management, Supply Chain Management usw., schwächen kann.

Wie entstehen die Schwachstellen?

Unzureichend gesicherte KI entsteht, wenn Sicherheitsprozesse vernachlässigt, Transparenzanforderungen ignoriert und Governance-Regeln nicht eingehalten werden. KI-Modelle werden in Produktivsystemen eingesetzt, ohne dass ihre Funktionsweise, Datenbasis oder Entscheidungslogik überprüft und dokumentiert wurde.

Low-Code-Tools und -Plattformen machen es möglich, dass auch weniger erfahrene Personen KI-Anwendungen erstellen – ein Innovationsvorteil, der aber auch die Angriffsfläche erhöht, wenn man sich zu 100% auf die Outputs der KI verlässt. In der Lieferkette werden oft Modelle und Daten von Dritten übernommen, ohne sich über Sicherheitsrisiken bewusst zu sein und einheitliche Sicherheitsstandards vorab zu implementieren.

Der Einsatz von KI im Bug Bounty Management, wo Meldungen automatisiert und dadurch zahlreicher, aber qualitativ schlechter werden, zeigt deutlich, wie herausfordernd es ist, zwischen echten Schwachstellen und Falschmeldungen zu unterscheiden. Insgesamt entsteht ein Flickenteppich aus Systemen, in denen niemand mehr den Überblick hat, wie, wo und mit welcher Integrität KI eingesetzt wird.

Positive Strategien für mehr Sicherheit

Die Risiken sind gross, aber es gibt zahlreiche Ansätze, wie Unternehmen und Privatpersonen diesen Herausforderungen konstruktiv begegnen können:

- **Transparenz schaffen:** Jede KI-Anwendung muss dokumentiert werden – inklusive Herkunft der Daten, eingesetzter Algorithmen und Entscheidungslogik. Nur so lassen sich Risiken nachvollziehen und kontrollieren.
- **Schulungen und Sensibilisierung:** Kontinuierliche Weiterbildung für alle Beteiligten ist essenziell. KI-Kompetenz darf nicht nur Expert*innen vorbehalten sein, sondern muss organisationsweit verankert werden.
- **Multidisziplinäre Teams:** Bei der Entwicklung und Einführung von KI sollten auch Teams aus IT, Recht, Ethik und anderen Fachbereichen eingebunden werden. So werden verschiedene Perspektiven und Kompetenzen genutzt, um Risiken frühzeitig zu erkennen.
- **Verantwortlichkeit und Governance:** Es sollten klare Verantwortlichkeiten für KI-Systeme benannt werden und Regeln für den Umgang mit KI definiert werden. Dazu gehört auch, dass Audits und Reviews durch unabhängige Stellen durchgeführt werden.

> « In einer Welt voller Low-Code-Chaos und KI-Automatisierung wird ein Bug-Bounty-Programm zum Seismografen für echte Risiken.

Antoine Neuenschwander
Head Bug Bounty

- **Fehlerkultur und Austausch:** Fehler und Sicherheitslücken sollten offen kommuniziert werden, um daraus zu lernen und Prozesse kontinuierlich zu verbessern. Ein transparenter Umgang mit Schwächen stärkt die gesamte Organisation.
- **Ethik und Nachhaltigkeit:** Neben technischen und wirtschaftlichen Kriterien muss jede KI-Anwendung auch unter ethischen und gesellschaftlichen Gesichtspunkten bewertet werden.
- **Nachwuchsförderung:** Die Nachwuchsförderung im Security-Bereich bleibt zentral. Juniors und Seniors müssen gemeinsam an Lösungen arbeiten – KI kann Kompetenz ergänzen, aber nicht ersetzen.

Mitarbeitende einbinden

Es ist wichtig, ethische, moralische und nachhaltigkeitsbezogene Aspekte rund um das Thema KI offen anzusprechen. Damit Mitarbeitende mit der rasanten Entwicklung von KI mithalten können, muss eine entsprechende Umgebung geschaffen werden. So lassen sich die Kompetenzen der Mitarbeitenden mittels gezielter Trainings stärken, beispielsweise durch Sensibilisierungsformate wie Promptathons.

Dies entspricht einem aktiven und bewussten Change-Management.

> «Wenn wir in Unternehmen ‹volle Kanne KI› geben wollen, dann braucht es vor allem eine Führung, die in der Digitalisierung Menschlichkeit vor Geschwindigkeit stellt. Kultur entsteht nicht durch Tools, sondern durch Vorbilder. Und bevor wir KI skalieren, müssen wir zuerst Menschen befähigen.

Marcus Beyer
Security Awareness Officer

Digitale Souveränität: Wer hat den letzten Rettungsring im Transformationsstrudel?

Ob im Alltag oder im Job: Die digitale Transformation ist längst überall angekommen und bringt für Unternehmen in der Schweiz ganz neue Spielregeln mit sich. Daten werden immer wichtiger, IT wandert in die Cloud und viele Prozesse laufen inzwischen extern. Genau deshalb steht das Thema digitale Souveränität aktuell so hoch im Kurs. Und die geopolitischen Veränderungen erhöhen die Dringlichkeit. Firmen müssen mehr denn je den Überblick über ihre Daten und digitalen Abläufe behalten – keine leichte Aufgabe in einer vernetzten Welt.

Doch was genau bedeutet digitale Souveränität eigentlich und warum ist sie gerade jetzt für Schweizer Unternehmen von so grosser Bedeutung? Während die Digitalisierung stetig voranschreitet und immer mehr Prozesse aus den Händen der Unternehmen in die Cloud oder zu externen Dienstleistern verlagert werden, steht die Frage im Raum, wie sich Organisationen ihre Handlungsfähigkeit und Kontrolle sichern können. Es braucht also ein klares Verständnis davon, was digitale Souveränität umfasst und welche konkreten Herausforderungen und Chancen damit verbunden sind.

Grundsätzlich gilt, dass Unternehmen und Organisationen immer in der Lage sein müssen, ihre digitalen Ressourcen – insbesondere Daten und IT-Infrastrukturen – eigenständig und unabhängig zu kontrollieren, zu steuern und zu schützen. Die Abhängigkeit von externen ausländischen Dienstleistern, insbesondere im Hinblick auf Cloud- und Outsourcing-Services, darf ein angemessenes Mass nicht überschreiten.

Für Schweizer Unternehmen ist digitale Souveränität aus mehreren Gründen relevant:

- Regulierungen wie das revidierte Schweizer Datenschutzgesetz (revDSG) und die europäische Datenschutz-Grundverordnung (DSGVO) verlangen, dass Unternehmen wissen, wo ihre Daten gespeichert werden und wer darauf Zugriff hat.
- Die Kontrolle über Daten und Systeme ist ein zentraler Faktor für die Informationssicherheit. Je mehr Abhängigkeiten von Dritten bestehen, desto grösser wird die Angriffsfläche.
- Wer seine Daten nicht kontrolliert, verliert im schlimmsten Fall den Zugang zu seinem wichtigsten Kapital und läuft Gefahr, Innovationskraft und Marktposition einzubüssen.

Outsourcing und Cloud: Kontrollverlust als Risiko – Illusion der Datensouveränität?

Die Auslagerung von IT-Diensten und die Nutzung von Cloud-Plattformen bieten enorme Vorteile in Bezug auf Skalierbarkeit, Kosten und Flexibilität. Gerade für Schweizer Unternehmen ist das Outsourcing an spezialisierte Anbieter oft wirtschaftlich sinnvoll. Gleichzeitig geht mit jedem Outsourcing-Schritt ein Teil der Kontrolle über Daten und Prozesse verloren.

Viele Unternehmen unterschätzen die Risiken, die mit der Abgabe von Daten an Drittanbieter einhergehen:

- **Abhängigkeit vom Anbieter:** Wechselkosten und technische Hürden machen es schwierig, den Anbieter zu wechseln oder zurückzuholen («Vendor Lock-in»).
- **Transparenzverlust:** Oft ist unklar, wo und wie Daten tatsächlich verarbeitet werden, insbesondere bei internationalen Cloud-Anbietern.
- **Rechtsunsicherheit:** Unterschiedliche Rechtsräume (z.B. durch Speicherung in der EU oder den USA) erschweren die Durchsetzung eigener Datenschutz- und Sicherheitsanforderungen.
- **Cybersecurity-Risiken:** Die Konzentration sensibler Daten in grossen Cloud-Plattformen macht diese zu attraktiven Angriffszielen für Cyberkriminelle.

Die vielbeschworene Datensouveränität bleibt in der Praxis oft eine Illusion – insbesondere dann, wenn Unternehmen nicht über die notwendigen Kontrollmechanismen und Kompetenzen verfügen, um ihre Datenflüsse und Abhängigkeiten zu steuern.

Die Schweiz verfügt mit dem revidierten Datenschutzgesetz (revDSG) seit September 2023 über eine der modernsten Datenschutzregulierungen Europas. Schweizer Unternehmen müssen die Prinzipien «Privacy by Design» und «Privacy by Default» umsetzen, Betroffenenrechte achten und Meldepflichten bei Datenschutzverletzungen erfüllen.

Besonders relevant ist die Frage, ob und wie Daten ins Ausland transferiert werden dürfen. Hier gelten strenge Vorgaben für die Übermittlung an Drittstaaten – insbesondere, wenn diese kein angemessenes Datenschutzniveau aufweisen. Für viele Unternehmen stellt sich damit die Frage, ob Cloud- und Outsourcing-Partner in der Schweiz oder im Ausland ansässig sein sollten.

> «Sich seiner digitalen Souveränität bewusst zu sein und diese aktiv zu steuern, ist heute für alle Unternehmen zwingend.

Lukas Hebeisen
Senior VP Cloud & Datacenter Solutions

Grosse Schweizer Anbieter wie Swisscom positionieren sich explizit als vertrauenswürdige Partner für digitale Infrastrukturen und bieten Cloud-Lösungen mit Datenhaltung in der Schweiz an. Damit adressieren sie die spezifischen Anforderungen an Datenschutz und Souveränität, die für viele Unternehmen entscheidend sind.

Neben der Datenhaltung in der Schweiz ist auch die Frage relevant, welchem Recht der Anbieter untersteht. Man sollte sich bewusst sein, dass US-Anbieter dem amerikanischen Recht unterstehen, selbst wenn die Daten in Schweizer Rechenzentren sind.

«Plus AI oder Minus AI?» – Auswirkungen auf die digitale Souveränität

Die aktuelle Debatte rund um künstliche Intelligenz wird zunehmend von einem Spannungsfeld geprägt, das sich grob in zwei Lager einteilen lässt: Plus AI – der optimistische Blick auf die technologischen Möglichkeiten – und Minus AI – der realistische bis kritische Blick auf Risiken, Abhängigkeiten und Kontrollverlust. Für Schweizer Unternehmen ist dieses Spannungsfeld besonders relevant, da es die Frage der digitalen Souveränität in bisher ungekanntem Ausmass beeinflusst.

Auf der einen Seite verspricht der Einsatz von KI enorme Vorteile: Automatisierung repetitiver Aufgaben, Effizienzsteigerung, datengetriebene Entscheidungsfindung und neue Innovationsmodelle. Unternehmen, die KI systematisch und verantwortungsvoll einsetzen, schaffen sich einen deutlichen Wettbewerbsvorteil und können ihre digitale Resilienz stärken. In diesem Kontext kann KI sogar ein Treiber für Souveränität sein – vorausgesetzt, Unternehmen behalten die Hoheit über ihre Daten, ihre Modelle und ihre Wertschöpfungsketten.

> «Digitale Souveränität entsteht dort, wo kritische Daten und Applikationen identifiziert werden und für sie vertrauenswürdige, lokale Lösungen gewählt werden. Das schliesst die Nutzung von innovativen globalen Diensten für weniger kritische Bereiche nicht aus.

Thomas Stemmler
Leiter Regulatory & Policy

Auf der anderen Seite verstärken KI-Technologien bestehende Risiken der digitalen Transformation. Mit jeder neuen Generation von KI-Systemen steigt die Abhängigkeit von grossen, oft internationalen Technologieanbietern. Modelle, Trainingsdaten, Infrastruktur und Wartung liegen häufig ausserhalb der direkten Kontrolle der Unternehmen. Die Gefahr von «Shadow AI», also die Verwendung von nicht autorisierten oder unkontrollierten KI-Tools im Arbeitsalltag, nimmt zu und untergräbt bestehende Governance-Strukturen. Dazu kommt die zunehmende Komplexität regulatorischer Vorgaben, die den rechtskonformen Einsatz von KI zusätzlich erschwert. In diesem «Minus AI»-Szenario wird digitale Souveränität schnell zur Herausforderung – oder gar zur Illusion.

Es ist nicht die Technologie, die darüber entscheidet, ob KI die digitale Souveränität stärkt oder schwächt. Vielmehr geht es um die Art und Weise, wie Unternehmen mit ihr umgehen. Bewusste Partnerwahl, transparente Datenflüsse, klare AI Governance, interne Kompetenzen und technische Schutzmechanismen sind entscheidend dafür, ob KI zu einem Souveränitätsgewinn oder zu einem Kontrollverlust führt. Unternehmen, die in diese Fähigkeiten investieren, können KI als strategischen Hebel nutzen – nicht nur für Effizienz und Innovation, sondern auch für den Schutz ihrer digitalen Unabhängigkeit.

Handlungsempfehlungen: Was können Unternehmen aktiv tun, um digital souverän zu bleiben?

Um digitale Souveränität nicht zur Illusion werden zu lassen, sollten Schweizer Unternehmen folgende Massnahmen ergreifen:

- **Strategische Steuerung:** Definieren Sie eine klare Digitalisierungs- und Datenstrategie, die auch den Umgang mit externen Dienstleistern und Cloud-Services regelt.
- **Risikobewertung und -management:** Analysieren Sie regelmässig die Risiken durch Outsourcing und Cloud-Nutzung und entwickeln Sie Notfallpläne für den Fall von Datenverlust oder -missbrauch. Bewerten Sie auch die Auswirkungen, wenn Sie kurzfristig den Zugang zu Ihren IT-Systemen verlieren oder wenn ein Hersteller kurzfristig die Rahmenbedingungen ändert.
- **Technische und organisatorische Massnahmen:** Nutzen Sie Verschlüsselung, Zugriffsmanagement und Monitoring, um Datenflüsse und Zugriffe transparent und kontrollierbar zu machen.
- **Vertragliche Absicherung:** Achten Sie auf klare vertragliche Regelungen zu Datenschutz, Datenzugriff, Datenportabilität und Exitstrategien beim Wechsel von Dienstleistern.
- **Partnerwahl mit Bedacht:** Setzen Sie auf Anbieter, die Datenhaltung und -verarbeitung in der Schweiz garantieren. Prüfen Sie regelmässig die Einhaltung der vereinbarten Standards.

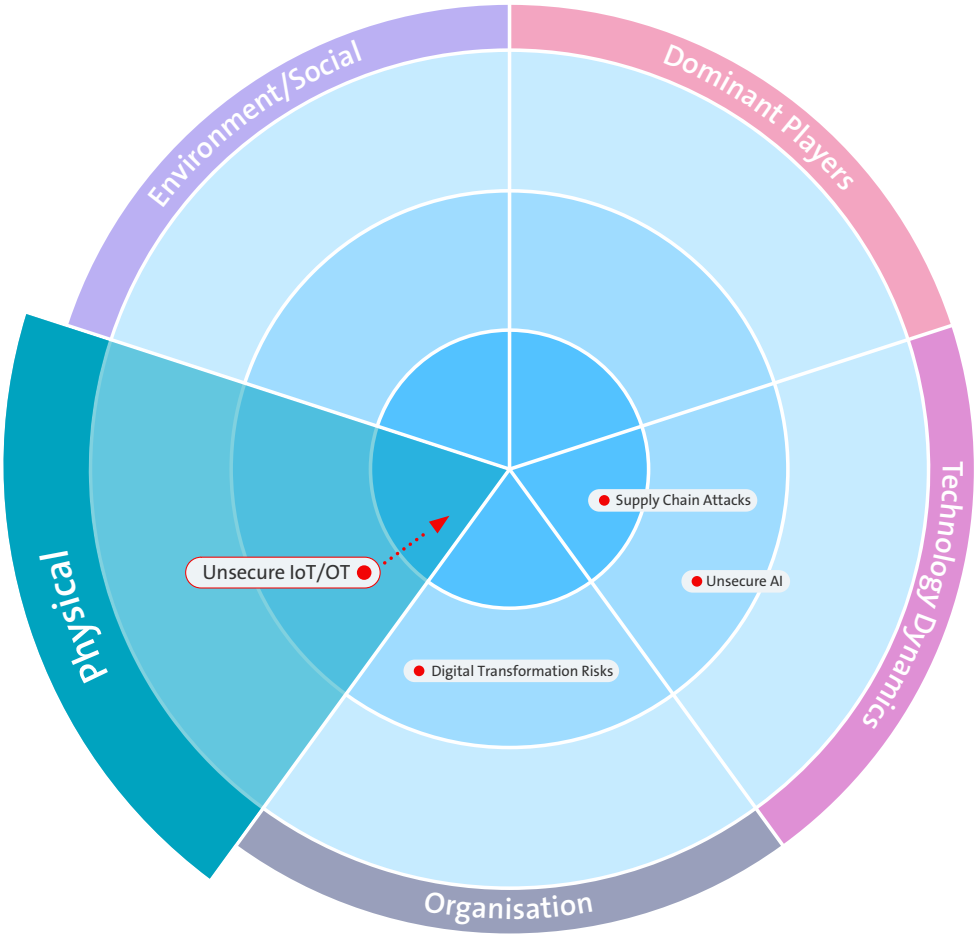
- **Schulung und Sensibilisierung:** Schulen Sie Mitarbeitende regelmässig im Umgang mit sensiblen Daten und den Risiken der digitalen Transformation.
- **Regulatorisches Monitoring:** Verfolgen Sie die Entwicklungen im Datenschutz und passen Sie Ihre Prozesse laufend an neue gesetzliche Anforderungen an.

Souveränität als Ziel

Die vollständige Kontrolle über alle digitalen Prozesse und Daten ist in einer globalisierten, digitalisierten Wirtschaft kaum realistisch. Digitale Souveränität bleibt ein anspruchsvolles Ziel, dem Unternehmen nur durch eine Kombination aus strategischer Steuerung, technischer Kompetenz und sorgfältiger Partnerwahl näherkommen können. Outsourcing und Cloud-Nutzung gehen nicht per se mit einem Kontrollverlust einher, vorausgesetzt, Unternehmen ergreifen die richtigen Massnahmen und managen ihre Risiken aktiv. Diese Aufgabe ist komplex und benötigt sehr spezialisiertes Wissen. Entscheidend ist, bewusst festzulegen, welche Kompetenzen intern aufgebaut und welche extern bezogen werden.

Wer sich der Risiken bewusst ist, proaktiv handelt und auf vertrauenswürdige Partner setzt, kann die digitale Transformation erfolgreich und sicher gestalten – und so im Transformationsstrudel nicht untergehen, sondern gestärkt daraus hervorgehen.

OT Security: der Elefant im Raum, der langsam sichtbar wird



Was haben Produktionsanlagen, Versorgungsinfrastrukturen, Verkehrssysteme, medizinische Geräte und Gebäudeautomation gemeinsam? Viele dieser für den Betrieb der Unternehmen wichtigen Systeme wurden aus Cyber-Security-Sicht in den letzten Jahren stark vernachlässigt – und sind nun vermehrt Bedrohungen ausgesetzt. Durch die fortschreitende Digitalisierung in der Produktion, das zunehmende Interesse von Cyberkriminellen an «leichter Beute» und die verändernde globale Sicherheitslage haben die Angriffe auf kritische Infrastrukturen zugenommen.

Die hieraus entstehenden Risiken für Unternehmen sind mannigfaltig: hohe Kosten durch beschädigte Maschinen, unbrauchbare Produktion, Reputationsschäden, Umweltschäden bis hin zu unmittelbaren Gefahren für Leib und Leben der Mitarbeitenden. Diese Risiken waren lange Zeit der sprichwörtliche Elefant im Raum, über den niemand so richtig sprechen wollte. Das ist vorbei, der Elefant wird zunehmend sichtbar und lässt sich nicht mehr ignorieren.

Operational Technology (OT) umfasst alle Systeme, die physische Prozesse steuern, überwachen sowie automatisieren und mit der realen Welt interagieren: von der Gebäudetechnik über Produktionsstrassen und Energieversorgungsnetze bis hin zu medizinischen Geräten im Spital. Mit der zunehmenden Vernetzung – Stichwort Industrie 4.0 und IoT – verschwimmen die Grenzen zwischen IT und OT immer stärker. Die Schnittstelle zwischen IT und OT ist der kritischste Punkt moderner Anlagenarchitekturen. Während in der IT das Paradigma der Vertraulichkeit dominiert, stehen in der OT die Verfügbarkeit und die unmittelbare Reaktionszeit an oberster Stelle. Ein Systemneustart nach einem Sicherheitsupdate, der in der IT Routine ist, kann in der OT zu einem Produktionsstopp führen, der einen direkten Einfluss auf die Bilanz haben kann.

Die grössten Herausforderungen sind:

- **Protokollvielfalt:** OT-Systeme nutzen oft proprietäre oder veraltete Protokolle, die ursprünglich nicht für die Vernetzung mit dem Internet konzipiert wurden.
- **Unterschiedliche Lebenszyklen:** Während IT-Hardware alle 3–5 Jahre erneuert wird, sind OT-Anlagen oft Jahrzehnte im Einsatz – inklusive veralteter Betriebssysteme, für die es keine Sicherheitspatches mehr gibt.
- **Malware-Transit:** Unsichere Schnittstellen ermöglichen es Ransomware, aus dem Office-Netzwerk direkt in die Steuerungsebene (SPS/PLC) überzugehen und die Produktion physisch zu manipulieren.
- **Der Air Gap bietet keinen absoluten Schutz:** Ein kompromittierter Techniker-Laptop genügt, um Schadcode direkt in das Herz der Produktion zu schleusen. Durch diesen direkten Zugang umgehen Angreifer klassische IT-Abwehrmechanismen und können Schwachstellen in industriellen Komponenten unmittelbar ausnutzen.

Historisch gewachsene OT-Systeme stammen aus einer Ära vor der Vernetzung. Sie basieren oft auf veralteter Software ohne moderne Authentifizierung, während starre Zertifizierungsprozesse notwendige Sicherheits-Patches blockieren. Das Ergebnis: Standard-IT-Sicherheitsmechanismen sind in diesen Umgebungen technisch oft nicht anwendbar oder können zu unkalkulierbaren Ausfällen führen.

Was steht für Unternehmen auf dem Spiel?

Die Risiken reichen von Produktionsausfällen durch Sabotage oder Manipulation bis hin zu Reputationsverlust und – in kritischen Infrastrukturen wie Energie, Wasser oder Gesundheitswesen – zur Gefährdung von Menschenleben. Auch rechtliche und regulatorische Konsequenzen sind zu beachten, denn die Nichteinhaltung von Sicherheitsvorgaben kann beträchtliche Bussgelder oder Haftungsrisiken nach sich ziehen.

Viele Unternehmen unterschätzen diese Gefahr, «weil bislang nichts passiert» ist. Doch gerade spektakuläre Angriffe wie Stuxnet, BlackEnergy und Colonial Pipeline oder die Angriffe auf Wasserkraftwerke in Polen und Norwegen beweisen, dass OT-Systeme im Visier von Hackern stehen und die Bedrohung sehr real ist.

Regulatorischer Druck

Der Gesetzgeber und die Regulierung nehmen die Gefahren für kritische Infrastrukturen zunehmend ernst. Beispiele hierfür sind die Aktualisierungen der Stromversorgungsverordnung der Schweiz, die eine Ausrichtung der Energieunternehmen am IKT-Minimalstandard vorschreibt. Oder die NIS2-Regulierung der EU, die auch für viele Schweizer Unternehmen mit Kunden in der EU Gültigkeit hat.

Was können Unternehmen tun?

Die gute Nachricht: Es gibt bewährte Ansätze, um die OT-Sicherheit zu verbessern. Identify, Protect, Detect, Respond und Recover – diese bekannten Schritte aus dem NIST Framework helfen und geben auch in der OT Security dem Ganzen eine Struktur.

Identify: Der erste Schritt ist – wie fast immer – Transparenz. Unternehmen sollten sich einen klaren Überblick verschaffen, welche OT-Systeme vorhanden sind, wie diese untereinander, mit der IT oder dem Internet kommunizieren und welches System kritische Schwachstellen aufweist. Ein solches kontinuierlich aktualisiertes Inventar ist die Basis für jegliches Risikomanagement.

Protect: Bestmögliche Trennung der OT von der IT, feingranulare Segmentierung im OT-Netz und – wo möglich – Endpoint Protection und Schwachstellenmanagement sind wichtige vorbereitende Massnahmen, um

> «Lange Lebenszyklen und proprietäre Systeme sind keine Ausrede mehr – mit zunehmender Vernetzung steigt die Verantwortung, OT-Systeme genauso konsequent zu schützen wie klassische IT.

Thomas Dummermuth
Head of Physical Security

Risiken zu minimieren. Hierzu gehört auch, den Zugriff auf OT-Systeme durch ein strin-gentes Access-Management zu limitieren.

Ein entscheidender Faktor ist die Sensibili-sierung der Mitarbeitenden. Wer die spezi-fischen Risiken und Best Practices kennt, kann im Alltag aktiv zur Sicherheit beitragen.

Detect: Parallel dazu ist ein kontinuierliches Monitoring sinnvoll. OT-Netzwerke sollten stets auf Unregelmässigkeiten und Angriffs-indikatoren überwacht werden, um im Ernst-fall schnell reagieren zu können. Hierfür sind auf OT spezialisierte IDS-Systeme verfügbar, die im Falle eines abnormalen Verhaltens einen Alarm auslösen. Die Definition des-sen, was als abnormal gilt, ist hochgradig industriespezifisch und benötigt entspre-chende Kompetenz beim Security-Partner.

Respond und Recover: Im Ernstfall benötigt es dann aber auch die Fähigkeit zu reagie-ren – auch ausserhalb der Bürozeiten. Ein konvergentes IT/OT-SOC ist ein hilfreicher Ansatz, der jedoch i.d.R. auch prozessuale Anpassungen im Unternehmen bedingt, wie z.B. Klärung von Verantwortlichkeiten oder Alarmierungsketten. Diese müssen auch mit den wichtigsten Lieferanten abgestimmt werden, um im Falle eines Falles eine zeit-nahe Wiederherstellung zu gewährleisten.

Um diese Schritte adressieren zu können, gilt es, die OT-, IT- und Managementebene eng in die Sicherheitsstrategie einzubinden. Das Management von OT-Security-Risi-ken gehört auf die Agenda der Geschäfts-leitung oder des Verwaltungsrates.

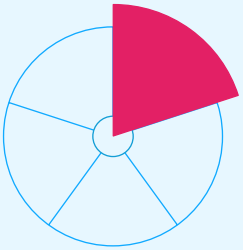
Die Zeit zu handeln ist jetzt

Die Vernachlässigung von OT Security ist keine Option mehr. Wer die Produktion in seinem Unternehmen auf dem Sicherheitsstand von gestern betreibt, riskiert nicht nur Produk-tionsausfälle und wirtschaftliche Schäden, sondern setzt auch seine Reputation und – im schlimmsten Fall – Menschenleben aufs Spiel. Die Herausforderung ist gross, aber lösbar. Entscheidend ist, dass Unternehmen das Thema proaktiv angehen und OT Security als integralen Bestandteil der digitalen Trans-formation verstehen. Der Elefant steht mitten im Raum – höchste Zeit, ihn anzusprechen und die richtigen Massnahmen zu ergreifen.

> « OT-Sicherheit heisst, die Vorteile der IT zu nutzen, ohne den stabilen Betrieb der Produktion zu gefährden. Entscheidend ist dabei die Schnitt-stelle zwischen IT und OT.

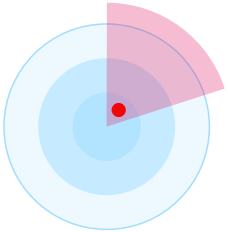
Tobias Balcon
Strategic Program Manager

Details inkl. Tendenzen und Vergleich zum Vorjahr



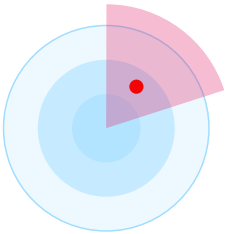
Dominant Players

In diesem Segment werden Bedrohungen subsumiert, die von Abhängigkeiten von dominanten Herstellern, Diensten oder Protokollen ausgehen.



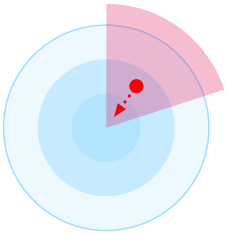
Infrastructure Integrity
In wesentliche Komponenten kritischer Infrastrukturen können fahrlässig oder bewusst Schwachstellen eingebaut worden sein, welche die Systemsicherheit gefährden.

- Unverändert



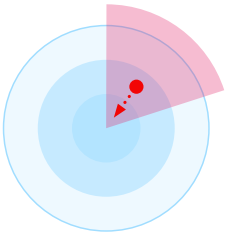
Legacy Protocols
Aufgrund von Softwareabhängigkeiten werden immer noch völlig veraltete, angreifbare Protokolle verwendet (z.B. NTLMv1, SMBv1, RC4), wodurch einige wenige Applikationen die Sicherheit ganzer Infrastrukturen gefährden.

► Unverändert



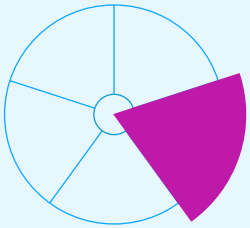
Cloud Ecosystem Dependencies
Zentrale Cloud-Ökosysteme erzeugen Klumpenrisiken und Abhängigkeiten, die bei Störungen oder politischem Druck die digitale Souveränität und Verfügbarkeit massiv beeinträchtigen können.

▲ Zunehmend



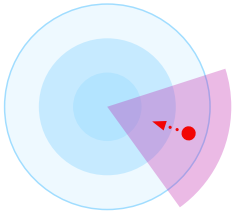
Manipulated Generative AI
Mit gezielten Manipulationen kann der Output eines KI-Systems verändert werden. Hier geht es um das Einschleusen von schlechten, falschen oder korrumpierten Daten bereits schon in der Trainingsphase, den Diebstahl von LL-Modellen, aber auch Prompt Manipulation, die zu unerwünschten und rechtlich bindenden Auswirkungen führen kann. Wir reden hier über AI Security Risks und nicht über Risiken durch die Nutzung von KI (siehe AI-Based Attacks).

▲ Zunehmend



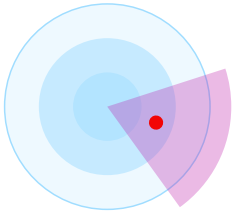
Technology Dynamics

Unter diesem Begriff sind Bedrohungen zu verstehen, die von der rasanten technologischen Innovation ausgehen und von der immer einfacheren und günstigeren Verfügbarkeit von IT-Medien und -Know-how profitieren. Das führt zu mehr Angriffsflächen, erhöht die Verfügbarkeit von Angriffswerkzeugen und bietet den Angreifern neue Möglichkeiten, durch die eigene Entwicklung neue Bedrohungen zu schaffen.



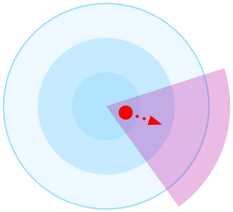
Quantum Computing
Quantencomputer können bestehende kryptografische Verfahren unbrauchbar machen, da sie diese in kürzester Zeit umgehen können.

▲ Zunehmend



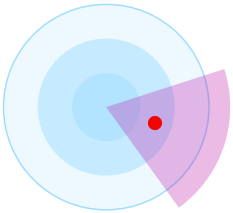
Unsecure AI
Unsichere KI-Systeme gefährden Lieferketten und den Datenschutz, da generative Modelle vertrauliche Daten unkontrolliert offenlegen können. Dadurch kann nicht nur die Geschäftskontinuität beeinträchtigt, sondern auch der Ruf eines Unternehmens erheblich geschädigt werden. Zudem drohen regulatorische Konsequenzen, insbesondere durch den AI Act, wenn KI-Entscheidungen gegen geltende Vorschriften verstossen.

► Unverändert



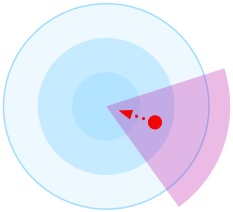
Ransomware
Kritische Daten werden grossflächig verschlüsselt und (möglicherweise) gegen Lösegeld wieder entschlüsselt.

▼ Abnehmend



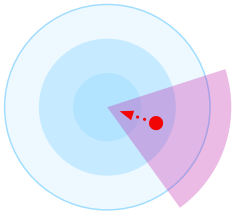
Increased Complexity
Die Komplexität von Systemen, insbesondere über Technologie- und Unternehmensgrenzen hinweg, nimmt laufend zu. Gerade im Hybrid-/Multi-Cloud-Umfeld mit vielen Cloud-Anbietern werden IT-Landschaften komplexer. Dadurch steigt die Risikoexposition und die Fehlersuche wird erschwert – Zero Day Exploits werden Tür und Tor geöffnet.

► Unverändert



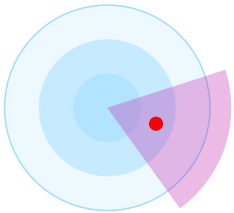
AI-Based Attacks
Angriffe mittels künstlicher Intelligenz (KI) sind gezielter und dadurch schwerer erkennbar. Durch KI können Angriffe effizienter mittels klassischer Angriffsvektoren wie Ransomware, Phishing und Spear-Phishing sowie vereinzelt auch mittels neuer Szenarien wie Deepfakes und Desinformation durchgeführt werden.

▲ Zunehmend



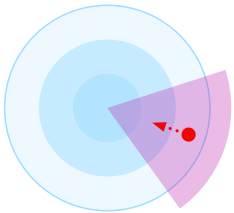
Agentic AI
Agentic AI ist proaktiv und in der Lage, eigenständig Entscheidungen zu treffen und Strategien anzupassen. Dadurch erhöht sich die Angriffsfläche, da selbstlernende und adaptive Systeme unvorhersehbare Verhaltensweisen entwickeln und selbstständig Interaktionen mit Umsystemen durchführen können. Bei einer Kompromittierung dieser Agents kann es zu unautorisierten Zugriffen auf sensible Daten und Systemkomponenten kommen, was die Wahrscheinlichkeit für Eskalation und Betrug drastisch erhöht. Auch eine scheinbar harmlose KI-Assistenz kann durch fehlerhafte Anweisungen oder Manipulation seitens der Angreifer erheblichen Schaden verursachen.

▲ Zunehmend



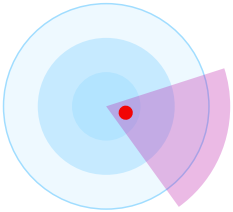
Targeted Attacks
Gezielte und komplexe Angriffe, um ein konkretes Ziel zu erreichen. Schlüsselpersonen werden identifiziert und gezielt direkt oder indirekt (Lateral Movement, Social-Engineering-Methoden) angegriffen, um relevante Informationen zu erhalten oder maximalen Schaden anzurichten. Ein wesentlicher Aspekt ist die Persistenz, d.h., dass die Angreifer möglichst lange unentdeckt agieren sowie ein Wechsel der Angriffskanäle (von Mail -> zu SMS -> zu Post) stattfindet.

► Unverändert



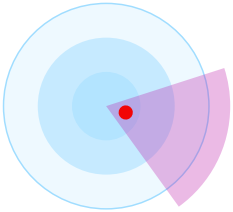
Subscriber Compromise
Schadsoftware verschafft sich Zugriff auf private Daten der Mobilnutzer*innen oder wird für Angriffe auf die Telekommunikations- bzw. IT-Infrastruktur genutzt. Phishing, Smishing, Vishing und MFA-Bypass-Angriffe zielen auf die Subscriber Credentials. Durch die Folgeattacken werden so ganze digitale Identitäten gestohlen und übernommen.

▲ Zunehmend



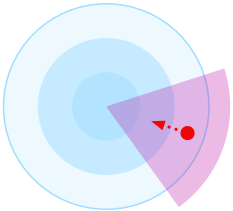
DDoS Attacks
Ein Distributed-Denial-of-Service-(DoS)-Angriff ist ein böswilliger Versuch, den normalen Datenverkehr eines Zielservers, -dienstes oder -netzwerks zu stören, indem das Ziel oder die umgebende Infrastruktur mit einer Flut von Internetverkehr überschwemmt wird. DDoS-Angriffe erreichen ihre Effektivität, indem sie mehrere kompromittierte Computersysteme als Quellen für Angriffsdatenverkehr nutzen. Ausgenutzte Maschinen können Computer und andere vernetzte Ressourcen wie IoT-Geräte umfassen. Starkes Wachstum bei geringem Schutz z.B. von IoT-Geräten führt zu mehr «Übernahmekandidaten» für Botnetze.

► Unverändert



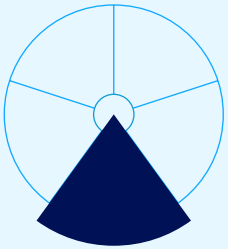
Supply Chain Attacks
Angriffe auf die Lieferkette zielen auf die Ausnutzung von Vertrauens- und Geschäftsbeziehungen zwischen einem Unternehmen und externen Parteien ab. Zu diesen Beziehungen können Partnerschaften, Lieferantenbeziehungen oder die Verwendung von Software Dritter gehören. Angriffe auf das Software-Ökosystem von Partnern erreichen in diesem Kontext eine neue Dimension.

► Unverändert



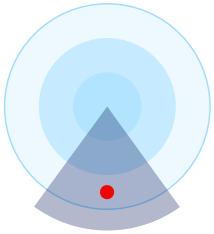
Residential Proxies
Residential Proxies sind Verbindungen über reale IP-Adressen, die genutzt werden, um den Ursprung von Datenverkehr zu verschleiern. Dadurch verlieren Sicherheitskontrollen, die auf IP-Reputation oder Geostandorte setzen, an Wirksamkeit. Das begünstigt Risiken wie Credential- und Informationsdiebstahl oder die Umgehung von Geoblocking. Auch die DDoS-Mitigation wird dadurch schwerer.

▲ Zunehmend



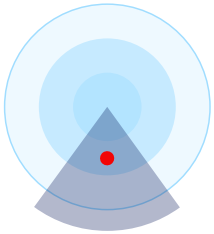
Organisation

Unter Organisation sind Bedrohungen zu verstehen, die von Veränderungen in Organisationen ausgehen oder Schwächen in Organisationen ausnutzen.



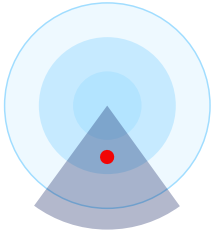
Workplace Heterogeneity
Neben den vielen Chancen, die neue Arbeitsmodelle mit sich bringen, führt der unkontrollierte Einsatz solcher Modelle, wie «Bring Your Own Device» (BYOD) oder der verstärkte Einsatz von Remote-Arbeitsplätzen, zu einer grösseren Risikoexposition.

- Unverändert



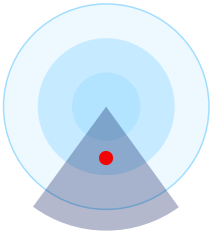
Decentralised Development & Operations
Klassische Entwicklungsabteilungen sterben aus und die Applikationsentwicklung rückt näher an die Business Units heran bei gleichzeitig kürzer werdenden Release-Zyklen. Dadurch wird die Kontrolle/Steuerung der Sicherheit erschwert.

- Unverändert



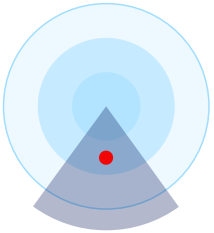
Insider Threat
Partner oder Mitarbeitende manipulieren, missbrauchen oder verkaufen Informationen fahrlässig oder vorsätzlich.

- Unverändert



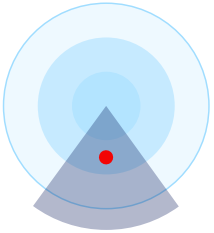
Digital Transformation Risks
Die immer stärkere Vernetzung der realen und der virtuellen Welt im Privat- und im Geschäftsleben führt zu mehr Angriffswegen. Auch das Konzept «New Work» und das Verschieben der Arbeit in Homeoffice-Umgebungen erhöhen das Cyberrisiko und die Angreifbarkeit der IT-Infrastruktur über ungesicherte Endgeräte.

► Unverändert



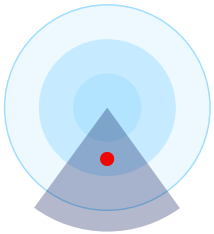
Security Skills
Durch die Komplexität der Cyberangriffe und die voranschreitende Digitalisierung werden Security Skills und der Einsatz von Cyber Professionals in der Organisation unabdingbar. Ein drohendes «Downskilling» – also das Verlernen von Wissen – durch Automatisierung in der IT kann zu neuen Angriffsvektoren führen, wenn z.B. SCADA-Anlagen nicht mehr durch die Fachkräfte bedient und gewartet werden können.

► Unverändert



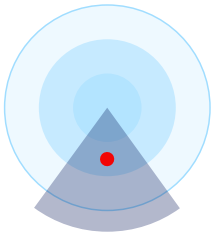
Fragile Workforce
Eine fragile Arbeitsorganisation beschreibt die Anfälligkeit von Cybersecurity- und Cyber-Defense-Teams für psychische Belastungen sowie fehlende Stress- und Burnout-Prävention. Wenn jemand psychisch instabil ist und nicht gut unter Druck handeln kann, erhöht sich die Wahrscheinlichkeit für menschliche Fehler. Dadurch entsteht ein erhöhtes Risiko für Sicherheitslücken und Angriffspunkte, die die Stabilität des gesamten Unternehmens gefährden können.

► Unverändert



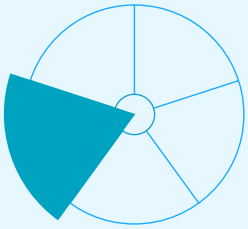
Infrastructure Misconfiguration
Ausnutzung von fehlkonfigurierten Infrastrukturkomponenten und/oder von Schwachstellen, die spät identifiziert und behoben werden. Bei einer stärkeren Automatisierung technischer Betriebsprozesse werden erfolgreiche Angriffe oder Fehlkonfigurationen grössere Auswirkungen haben.

► Unverändert



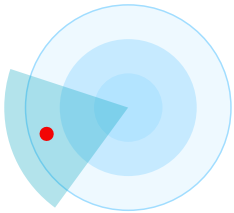
Fraud
Fraud bezeichnet betrügerische Handlungen, die auf Täuschung und unrechtmässiger Bereicherung basieren. Er äussert sich in gefälschten Transaktionen, Identitätsdiebstahl oder manipulierten Dokumenten. Für Unternehmen und Privatpersonen stellt Fraud eine erhebliche Gefahr dar, da er zu finanziellen Verlusten und Reputationsschäden führen kann.

► Unverändert



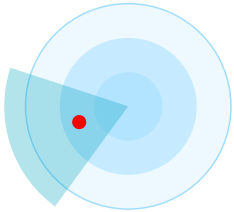
Physical

Unter diesen Begriff fallen Angriffe auf die Infrastruktur im Cyberspace, die vermehrt Schaden in der physischen Welt verursachen. Aber auch Bedrohungen, die von der physischen Umgebung ausgehen und in der Regel eher auf physische Ziele ausgerichtet sind, zählen dazu.



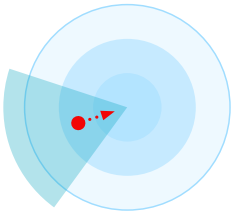
Energy Instability
Angriffe auf kritische Infrastrukturen wie Stromnetzbetreiber. Die Ausfallsicherheit ist essenziell und Business Continuity wird verstärkt auch in der Cyberresilienz-Debatte thematisiert. Strommangellage, Blackout (flächendeckender Stromausfall) oder gar Blueout (flächendeckender Ausfall der Wasserversorgung) u. Ä. sind wichtige Punkte. Den Medien ist zu entnehmen, dass die Verwundbarkeit kritischer Infrastrukturen durch Cyberangriffe stark zugenommen hat.

► Unverändert



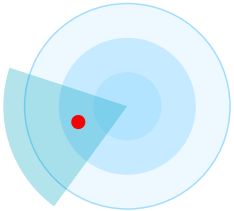
Targeted Sabotage
Es geht um die gezielten Attacken auf wichtige kritische Infrastrukturen, Versorgungsanlagen und Leitungen, was zu beachtlichen Einschränkungen im Internet führt. Die gezielte Sabotage von neuralgischen Glasfaserkabeln nimmt zu, ist eine Gefahr und muss beobachtet werden. Gegenmassnahmen sind schwierig umzusetzen, es ist auf eine rasche Detektion und Ausweichlösungen zu setzen.

► Unverändert



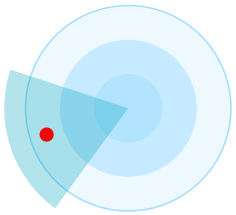
Unsecure IoT/OT
Ob Betriebstechnologie (OT) zur Überwachung und Steuerung von physischen Prozessen, Geräten und Infrastrukturen oder IoT-Geräte – das Internet der Dinge ist immer und überall. Dabei werden hier verschiedenste Aufgaben – von simpel bis komplex – erfüllt, die von Home-Entertainment-Anwendungen über die Steuerung von Robotern in einer Werkshalle bis zur Überwachung kritischer Infrastrukturen (CI) reichen. Schwach geschützte Geräte – welcher Art auch immer – können kompromittiert und sabotiert werden. So können sie in der eigenen Funktion, z.B. in der Verfügbarkeit oder Datenintegrität, eingeschränkt werden.

▲ Zunehmend



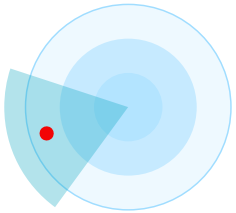
Environmental Influence
Durch die Auswirkungen des Klimawandels und der Urbanisierung treten vermehrt unvorhersehbare Wetterphänomene und Wettereinflüsse wie Hitze, Starkregen, Tornados, Hagel, höhere Blitzintensitäten u.ä. auf, welche Auswirkungen auf die Infrastrukturresilienz und damit ein hohes Schadenspotenzial in Bezug auf die externe und interne Umgebung eines Informationssystems oder Netzwerks haben.

► Unverändert



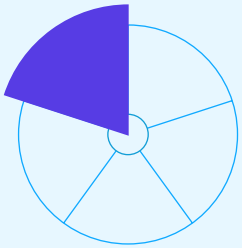
UAS Threats
UAS Threats (Unmanned Aerial System Threats) bezeichnen Risiken, die durch den Einsatz unbemannter Luftfahrzeuge – also Drohnen – entstehen. Diese reichen von Spionage, Überwachung und Datendiebstahl über Schmuggel und Sabotage bis hin zu physischen Angriffen auf Infrastruktur oder Personal. Im Unternehmenskontext sind insbesondere Industriespionage, Luftüberwachung von Werksgeländen und Störung sensibler Anlagen relevante Szenarien. Mit der zunehmenden Verbreitung und Autonomie von Drohnentechnologien nimmt die sicherheitsrelevante Bedeutung dieses Threats deutlich zu.

- Unverändert



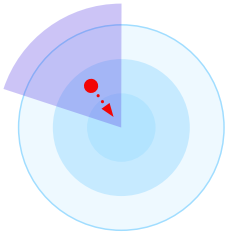
Hybrid Warfare
Die Kombination klassischer militärischer Mittel mit nicht militärischen Taktiken wie Cyberangriffen, Desinformation, wirtschaftlichem Druck oder politischer Einflussnahme wird als hybride Kriegsführung bezeichnet. Weil Angriffe oft verdeckt und unterhalb der «Kriegsschwelle» erfolgen, ist sie schwer zu erkennen und abzuwehren. Ziel ist es, Staaten zu destabilisieren, Vertrauen zu untergraben und gesellschaftliche Spaltung zu fördern. Ihre Wirksamkeit steigt durch Digitalisierung, soziale Medien und globale Vernetzung.

- Unverändert



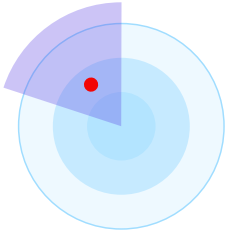
Environment/Social

Damit sind Bedrohungen gemeint, die von gesellschaftspolitischen Änderungen ausgehen oder durch solche Änderungen einfacher zu missbrauchen sind und dadurch für Angreifer wertvoller werden.



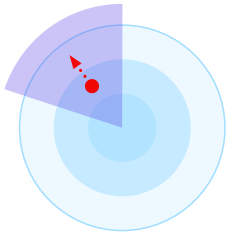
Identity Theft & Impersonation
Beglaubigte, persönliche digitale Identitäten können gestohlen oder missbraucht werden, um sich als eine andere Person oder Organisation auszugeben. Dies ermöglicht Angreifern, unbefugt auf Systeme und Informationen zuzugreifen oder im fremden Namen Handlungen wie Vertragsabschlüsse, Zahlungen oder Kommunikationsvorgänge durchzuführen.

▲ Zunehmend



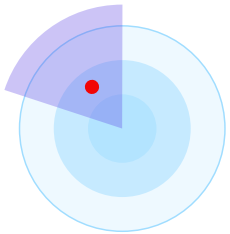
Geopolitical Situation / State Level Attacks
In Zeiten von Kriegen, Terror und politischer Instabilität von Ländern und Gesellschaften lassen sich zunehmend auch negative Folgen im Cyberraum erkennen. Hierbei handelt es sich um Auftragshacks von unterschiedlichen Ländern und politisch motivierten Hacktivist*innen, staatlichen Akteur*innen und organisierten Kriminellen die zunehmend Druck auf Unternehmen und Organisationen durch Auftragsarbeiten ausüben. Auch Kollateralschäden durch Hack-Back-Strategien einzelner Länder wird hier vermehrt Beachtung geschenkt.

► Unverändert



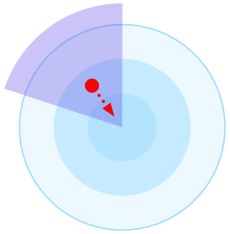
Security Job Market
Der Bedarf an Security Professionals ist enorm gross und kann nur sehr schwer gedeckt werden. Dies führt zu einem abnehmenden Know-how im Kampf gegen immer komplexere und intelligentere Angriffe.

▼ Abnehmend



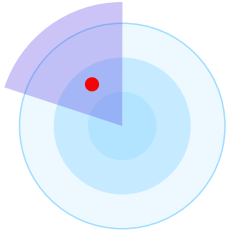
Disinformation & Destabilisation
Die absichtliche Verbreitung von unwahren Informationen kann zu einer wirtschaftlichen und gesellschaftlichen Destabilisierung führen und wird gerade in Krisenzeiten vermehrt auch über den Cyberraum gezielt eingesetzt.

► Unverändert



Political Influence
Politische Strömungen, aber auch Regularien und Vorgaben können Einfluss auf technologische oder wirtschaftliche Entscheide nehmen, z.B. bei der Auswahl von Technologielieferanten. Daraus können neue Risiken entstehen. Auch Data Sovereignty – also Datensouveränität bzw. Datenhoheit aus staatlicher Sicht – hat einen Einfluss darauf.

▲ Zunehmend



Data-Centric Risks
Mehr Daten und bessere Analysemodelle können missbraucht werden, um das Verhalten von Menschen zu beeinflussen. Entscheidungen werden vermehrt autonomen Systemen überlassen. Daten aus Big Data Lakes werden gezielt für Desinformation, Fake News, gesellschaftliche und psychosoziale Analysen sowie die Erstellung von Bewegungsmustern herangezogen. Mit Letzterer geht eine Verletzung der Privatsphäre einher.

► Unverändert

Fazit

Die digitale Transformation führt zu einer immer stärkeren Abhängigkeit von externen Ökosystemen.

Cloud-Plattformen, Software-Lieferketten, KI-Modelle und industrielle Steuerungssysteme sind hochgradig vernetzt und häufig ausserhalb der direkten Kontrolle der Unternehmen. Damit verschieben sich klassische Sicherheitsgrenzen. Vertrauen allein genügt nicht mehr – Sicherheit muss nachvollziehbar, überprüfbar und steuerbar sein. Herkunft, Integrität und Abhängigkeiten von Software, Daten und Systemen müssen transparent gemacht und aktiv gemanagt werden.

Besonders deutlich zeigt sich dies bei Supply-Chain-Angriffen und der digitalen Souveränität. Wer nicht weiss, wie Software entsteht, wo Daten verarbeitet werden oder welchen rechtlichen Rahmenbedingungen Anbieter unterliegen, riskiert einen Kontrollverlust mit potenziell gravierenden Folgen für das gesamte Unternehmen. Regulatorische Entwicklungen wie NIS2 und CRA oder Datenschutzgesetze verstärken diesen Druck zusätzlich und machen überprüfbare Sicherheit zum Standard.

Künstliche Intelligenz wirkt dabei als Beschleuniger. Sie kann Produktivität, Innovation und Resilienz steigern, verstärkt aber bei fehlender Governance bestehende Risiken entlang der gesamten Wertschöpfungskette. Intransparente Modelle, Shadow AI, Kompetenzverlust und neue Angriffsflächen machen deutlich: Entscheidend ist nicht der Einsatz von KI an sich, sondern die Art und Weise, wie sie eingeführt, kontrolliert und verantwortet wird.

Ein oft unterschätzter, aber kritischer Bereich bleibt die OT und IoT Security. Die zunehmende Konvergenz von IT und OT macht Produktionsanlagen und kritische Infrastrukturen zu attraktiven Zielen. OT Security sollte nicht mehr als technische Randdisziplin behandelt werden – das Thema gehört auf die Agenda der Geschäftsleitung.

Das Bedrohungsbild 2026 zeigt, dass Risiken zunehmend im Zusammenspiel von Technologie, Organisation und Geopolitik entstehen. Resilienz wird zur Schlüsselkompetenz – technisch, organisatorisch und kulturell.

Die grössten Gefahren entstehen dort, wo Komplexität auf fehlende Transparenz, Automatisierung auf fehlende Verantwortung und Tempo auf mangelnde Kompetenz treffen. Die Antwort darauf ist kein einzelnes Tool, sondern ein ganzheitlicher Ansatz. Es braucht klare Strategien, eine überprüfbare Sicherheit, eine bewusste Partnerwahl, kontinuierliche Weiterbildung und eine Sicherheitskultur, die von Führungskräften aktiv und glaubwürdig vorgelebt wird.

Die im aktuellen Cybersecurity Threat Radar identifizierten Entwicklungen machen deutlich, dass Cybersecurity längst nicht mehr nur eine technische Disziplin, sondern ein strategischer Erfolgsfaktor ist. Cybersecurity ist kein Zustand, sondern ein kontinuierlich strategischer Prozess. Wer ihn aktiv gestaltet, stärkt Resilienz, Vertrauen und digitale Souveränität.

#EngageYourSecuritySkills

Impressum

Herausgeberin
Swisscom (Schweiz) AG, Group Security

Konzept / Realisation
Agentur Nordjungs, Zürich

Redaktion
Swisscom (Schweiz) AG
Marcus Beyer (Group Security)
Manuel Bühlmann (Group Communications)
Claudia Lehmann (B2B Communications)

Druck
OK DIGITALDRUCK AG, Zürich

Auflage
140 Exemplare

Cybersecurity entscheidet heute über Vertrauen und Handlungsfähigkeit, denn digitale Transformation, KI und geopolitische Abhängigkeiten lösen Sicherheitsgrenzen auf und machen transparente, überprüfbare Sicherheit sowie ganzheitliche Resilienz zur strategischen Pflicht.

Mehr zu unseren Produkten, Dienstleistungen und dem Engagement für Sicherheit in der Schweiz finden Sie unter: swisscom.ch/sicherheit

Interesse an einem Job im Security-Bereich bei Swisscom? Dann bewirb dich hier: swisscom.ch/securityjobs

#EngageYourSecuritySkills