Cyber Security Threat Radar 2023/2024

Cyberresilienz stärken

swisscom

Inhalt

Cyber Security Threat Radar

Cyberresilienz stärken

Gerade in diesen turbulenten und anspruchsvollen Zeiten ist es für Unternehmen und Organisationen entscheidend, widerstandsfähig zu sein. Dies umfasst nicht nur die physische Gesundheit und stabile, redundante IT-Systeme, sondern beinhaltet auch klare Richtlinien, die als Leitplanken für mehr Orientierung sorgen.

Der vorliegende Cyber Security Threat Radar verdeutlicht, dass der Schutz vor Cybergefahren und die Risikominderung kein einseitiger Prozess sind und auch nicht ausschliesslich in der Verantwortung der IT liegen. Cybersicherheit ist Chefsache und erfordert die Beteiligung der gesamten Unternehmensführung.

Im diesjährigen Cyber Security Threat Radar verzichten wir auf die Behandlung des vierten Sektors der Cyberbedrohungen: Beobachtung. Dieses Thema ist bereits integraler Bestandteil unserer Swisscom Security-DNA und wird täglich in unserer Arbeit berücksichtigt.

Im vorliegenden Radar wird «Disinformation & Destabilisation» als eine der bedeutendsten Herausforderungen unserer Zeit identifiziert. Die Verbreitung von falschen Informationen, manipulierten Inhalten und gezielten Propagandaaktionen kann ganze Gesellschaften beeinflussen, politische Prozesse stören und das Vertrauen in Institutionen untergraben. Auch die Expert*innen des Global Risks Report 2024 des World Economic Forum (WEF) stufen diese Bedrohung als das grösste kurzfristige Risiko ein. Die Themen im Radar sind sicher nicht abschliessend.

Mit dem im September letzten Jahres revidierten Datenschutzgesetz in der Schweiz und dem neuen Informationssicherheitsgesetz (ISG) rücken Governance-Aspekte wieder stärker in den Vordergrund. Wir sind gespannt, was die Zukunft bringt. Ich hoffe, dass Ihnen der vorliegende Cyber Security Threat Radar wertvolle Inputs liefert und Ihnen dabei hilft, die Cybersicherheit in Ihrem Unternehmen oder Ihrer Organisation weiter voranzubringen.

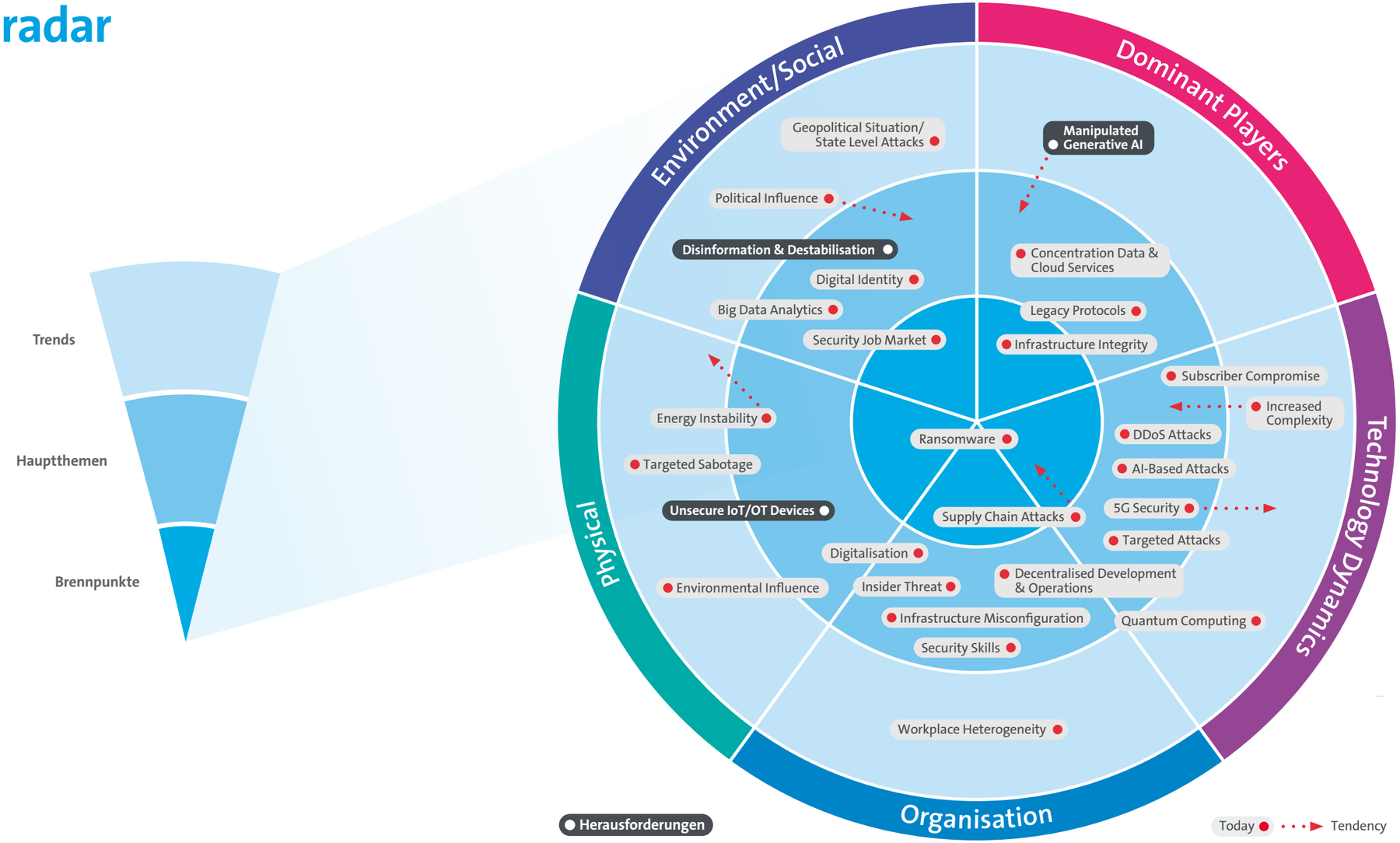
Marco Wyrsch
Head of Group Security
Swisscom (Schweiz) AG

« Monitoring und Observation unseres Netzes – so machen wir die Schweiz kontinuierlich ein ganzes Stück sicherer. Denn Cyberrisiken bleiben eines der Top-Risiken der kommenden Jahre für Organisationen, Unternehmen und die Gesellschaft im Allgemeinen. »

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 Cyber Security Threat Radar.



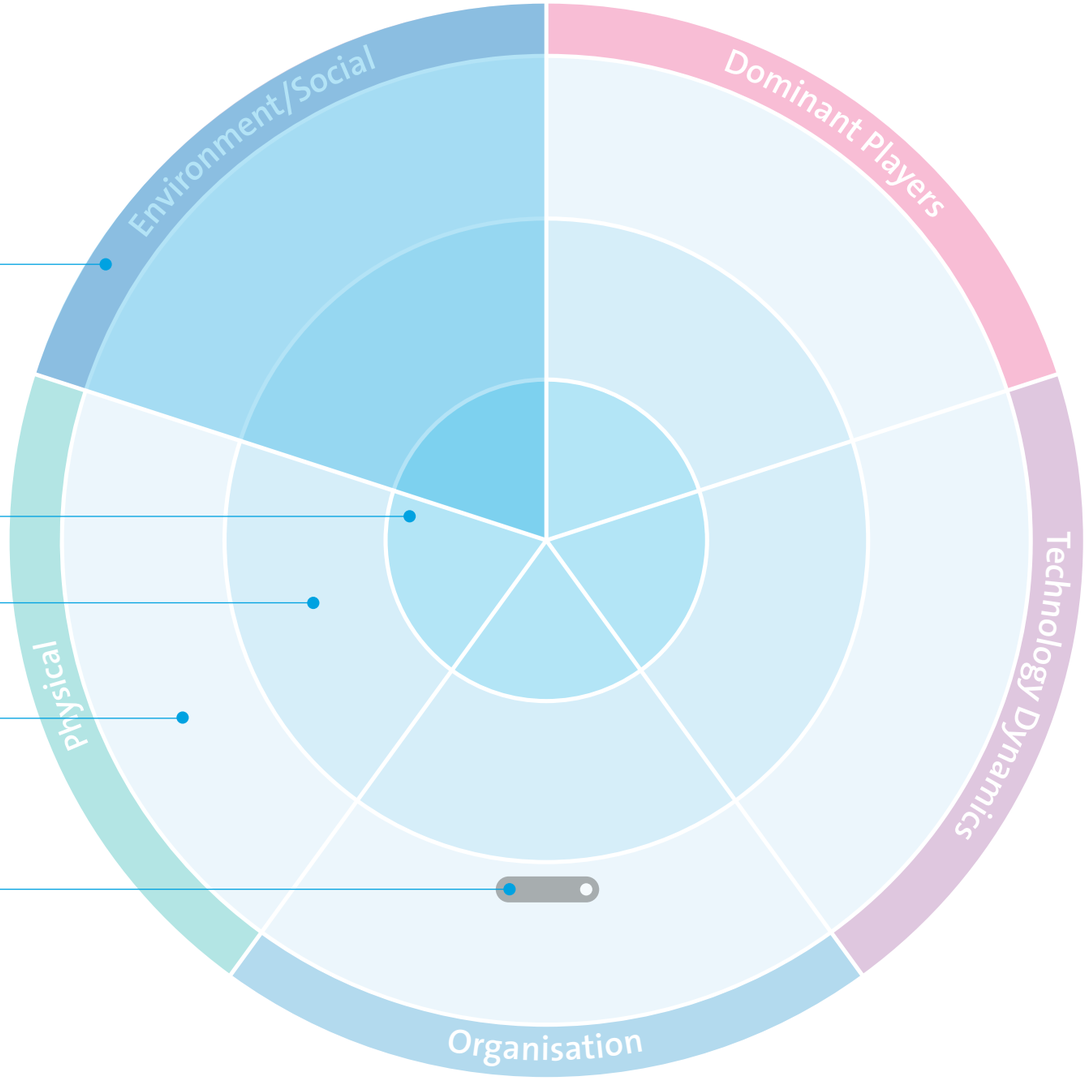
Methodik

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.

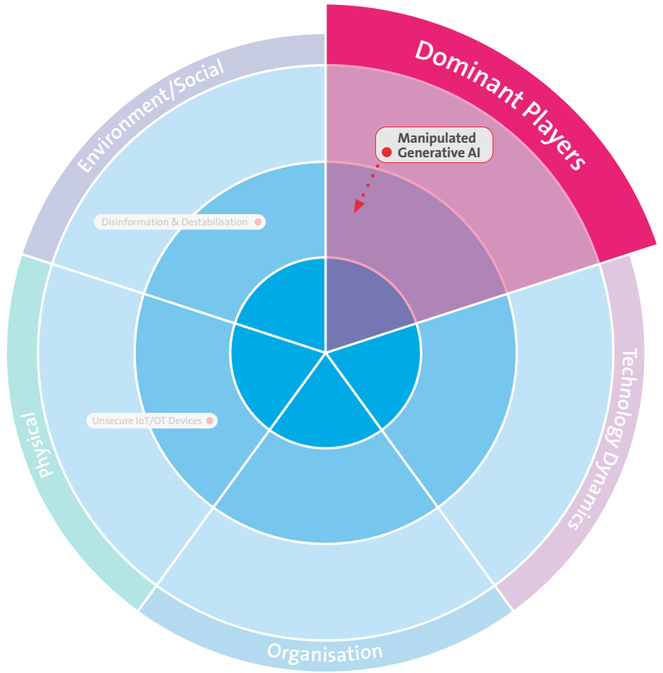
Die Kreise kennzeichnen wir als:

- **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.



Manipulated Generative AI oder: Wie manipulierbar ist die künstliche Intelligenz?



Digitalisierung, Virtualisierung und der Cloud-Trend waren in der IT in den letzten 15 Jahren von grosser Bedeutung und haben ihren Teil zur raschen Verbreitung von Generative AI beigetragen. Die Veröffentlichung von ChatGPT im November 2022 wurde von einem gewaltigen Medienecho begleitet. Generative AI ist schnell in der Gesellschaft angekommen. Viele innovative Unternehmen liessen sich von der Begeisterung anstecken und bringen seither zahlreiche neue Anwendungen auf den Markt.

Das weltweite Interesse an KI rückte das Thema auch stärker in das Blickfeld der Security. Fragen bezüglich Sicherheitsrisiken wurden schnell laut und wollten beantwortet werden – denn wie immer gibt es bei Innovationen auch Schattenseiten. Trotz der bedeutenden Fortschritte, die KI und maschinelles Lernen gemacht haben, sind diese Technologien anfällig für Angriffe. In vielen Teilbereichen befinden sich neue Standards erst in der Entwicklung, wie beispielsweise der AI Act in der Regulierung. Es ist also mit einigen Unbekannten zu rechnen, auf die man sich nur bedingt vorbereiten kann.

Es gibt drei Aspekte, bei denen KI-Systeme im Kontext von Cybersicherheit sichtbar sind:

1. Verwendung von KI-Systemen für Angriffe: Bekannte Beispiele sind hier die Verfeinerung bekannter Angriffe wie CEO Fraud und Business Email Compromise (BEC) mittels AI-generierter Videos anstelle von einfachen E-Mails; realistischere Phishingmails → AI-based Attacks.

2. Einsatz von AI zur Erkennung und zur Abwehr von Angriffen (z. B. bei Spam- und Phishingfiltern), in der Anomalieerkennung im Netzwerkverkehr, der Workflow-Unterstützung in der Cyber Defence (z. B. als Copilot), bei der Automatisierung von Analyseschritten, der Erstellung von Incident Timelines oder der Kommunikation mit Benutzern. Insgesamt ist hier mit weiteren intelligenten und automatisierten Security-Lösungen zu rechnen.

3. Sicherheitslücken in eingesetzten AI-Systemen – und hier reden wir von manipulierbarer künstlicher Intelligenz, konkret zu finden in den:
   OWASP Top 10 for LLM (owaspai.org) und/oder dem MITRE ATLAS (atlas.mitre.org).
   Es geht hier also um AI Security Risks und nicht um Risiken durch die Nutzung von KI-Systemen.

Beim dritten Aspekt sind aus unserer Sicht – neben zahlreichen weiteren Angriffsmöglichkeiten – insbesondere die folgenden Themen von Relevanz:

- **Manipulation von Inputs (z. B. Prompt Injections)**
  Bei diesen Angriffen wird versucht, über eine Manipulation der Eingaben bestehende Sicherheitsmechanismen zu umgehen und damit durch den Betreiber des KI-Systems unbeabsichtigte Ergebnisse zu produzieren. Dabei kann es sich beispielsweise um die Bekanntgabe vertraulicher Informationen oder die Generierung von unerwünschten Inhalten oder unerwünschtem Verhalten handeln.

- **Poisoning-Angriffe**
  Bereits schon in der Trainingsphase von KI-Systemen kann durch das Einschleusen von schlechten, falschen oder korrumpierten Daten das System manipuliert werden. Ein Beispiel wäre das Einfügen unangemessener Sprache in Audioaufzeichnungen, sodass ein Chatbot diese Fälle als allgemein genug interpretiert, um sie in Kundeninteraktionen zu verwenden.

- **Supply Chain Attacks**
  Hier handelt es sich um Angriffe, die sich gegen externe Komponenten des AI-Systems richten. Ein Beispiel wäre das Einschleusen von Schadcode in Open-Source-Bibliotheken, welche in einem KI-Modell verwendet werden.

Daneben besteht auch weiterhin das Risiko von DoS (Denial of Service). Ein Benutzer könnte zum Beispiel absichtlich oder unabsichtlich mit einer Eingabe alle Ressourcen aufbrauchen und das System lahmlegen.

Kurz zu erwähnen sind auch andere KI-Risiken, wie beispielsweise «Schatten-KI» (Shadow AI), bei welcher Mitarbeitende unkontrolliert KI-Systeme verwenden und dadurch die Geheimhaltung von Unternehmens-, Kunden- oder sonstigen schützenswerten Daten gefährden. Dadurch wird die Datensicherheit gefährdet. Es muss sichergestellt werden, dass die geheim zu haltenden Firmendaten geschützt sind und das KI-System vertrauenswürdig ist.

« Wegen der probabilistischen Eigenschaften von GenAI und LLMs stehen wir vor neuen Security-Herausforderungen und -Risiken. Ein tiefgründiges Verständnis, wie LLMs funktionieren, ist Voraussetzung, um die richtigen Security-Massnahmen zu definieren und umzusetzen. »

Beni Eugster
Swisscom Outpost

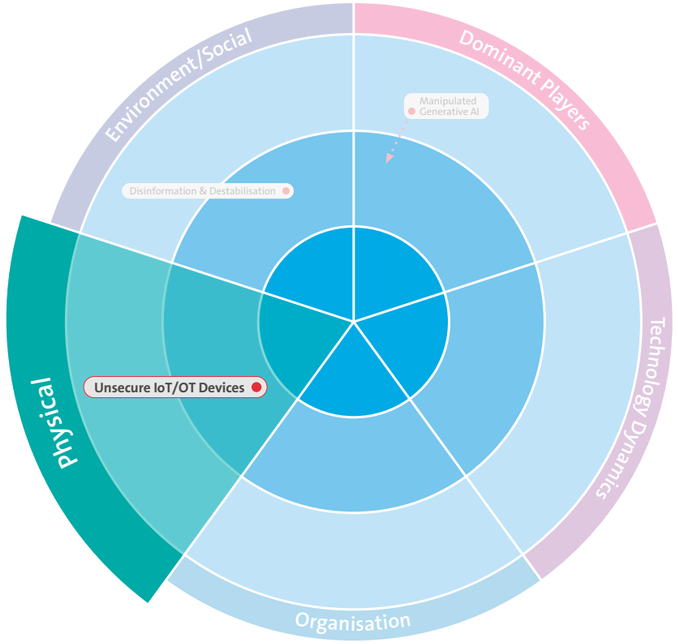
Darauf sollten Unternehmen und Organisationen im Umgang mit den Risiken von künstlicher Intelligenz ihren Fokus legen:

- Beobachtung der aktuellen Entwicklungen und schnelle Reaktion bei Änderungen.
- Schulung von Mitarbeitenden.
- Sorgfältige Risikoanalyse vor dem Einsatz von AI-Systemen (auch von Dritten) betreffend mögliche Auswirkungen.
- Prüfen und Umsetzen von Sicherheitsmassnahmen auf allen Stufen des AI Lifecycle. Betrachten Sie Sicherheitskontrollen von NIST AI RMF, MITRE ATLAS und OWASP für AI-Sicherheit.
- Gute Beziehungen zwischen AI und Security Teams pflegen. Regelmässige Anpassungen von Regelwerken und Vorgaben aufgrund neuer Entwicklungen durchführen.
- Erarbeitung von Handlungsanweisungen für den Umgang mit AI in der eigenen Organisation.
- Rechtliche Rahmenbedingungen: Der AI Act fordert bereits besondere Sicherheitsmassnahmen für riskante AI-Systeme oder schränkt deren Verwendung ein. Die KI-Verordnung der EU hat eine extraterritoriale Wirkung und gilt damit unter bestimmten Voraussetzungen auch für Schweizer Unternehmen. Aber auch das Urheberrecht und die Haftung bei Verwendung von AI-Systemen Dritter als SaaS-Lösung sind Risiken, die nicht vergessen werden sollten.

« Die Herausforderungen im Umgang mit AI Security Risks werden durch die rasante Entwicklung im AI-Umfeld zunehmen. Und zwar mit hoher Geschwindigkeit. Hier sollte man die aktuellen Entwicklungen kontinuierlich beobachten, um schnell auf Änderungen reagieren zu können. »

Raiko Zwilling
Security Officer Group Companies

Sicherheitsrisiken durch die zunehmende Digitalisierung auch in der Werkhalle und im OP-Saal



In der heutigen komplexen und vernetzten Welt spielen Geräte für das IoT (Internet of Things) und OT (Operational Technology) in verschiedenen Bereichen eine zentrale Rolle im Arbeitsalltag. Dabei erfüllt die Technologie eine Vielzahl von Aufgaben, sowohl einfache als auch komplexe – von Home-Entertainment- und Smart-Home-Anwendungen über die Steuerung von Fertigungssystemen in Industriebetrieben bis hin zur Überwachung kritischer Infrastrukturen.

Allerdings birgt die zunehmende Vernetzung dieser Geräte auch signifikante Sicherheitsrisiken. Unsichere oder schwach geschützte IoT/OT-Geräte können kompromittiert und sabotiert werden und so zum Einfallstor für Cyberangriffe werden. So können sie in der eigenen Funktion, z. B. der Verfügbarkeit oder der Datenintegrität, nicht nur eingeschränkt werden, sondern auch die physische Sicherheit und das Wohl der Menschen bedrohen. Die Sicherheit von IoT/OT-Systemen ist also von entscheidender Bedeutung, da Angriffe auf diese Systeme zu erheblichen Schäden führen können.

Die Risiken unsicherer IoT/OT-Geräte sind vielfältig und können je nach Anwendungsbereich variieren. Zu den Hauptgefahren gehören:

- **Betriebsunterbrechungen**
  Eine Sicherheitsverletzung kann dazu führen, dass kritische Systeme vorübergehend oder dauerhaft ausser Betrieb sind, was erhebliche Produktionsausfälle und finanzielle Einbussen zur Folge haben kann.

- **Diebstahl geistigen Eigentums bzw. Datenverlust oder -diebstahl**
  Unautorisierte Zugriffe auf IoT/OT-Geräte können den Diebstahl von sensiblen Daten, einschliesslich geistigen Eigentums und Betriebsgeheimnissen, zur Folge haben, was den Wettbewerbsvorteil eines Unternehmens schwächen und zu Datenschutzverletzungen wie auch finanziellen Verlusten führen kann.

- **Manipulation von Gerätedaten und Sabotage**
  Angreifer können Daten von IoT/OT-Geräten manipulieren, um falsche Informationen zu produzieren, die zu fehlerhaften Entscheidungen oder Produkten führen können. In industriellen Umgebungen können Angreifer kritische Infrastrukturen lahmlegen oder manipulieren, was Ausfälle und sogar Gefahren für die menschliche Sicherheit zur Folge haben kann.

- **Netzwerkinfiltration**
  Einmal kompromittiert, können IoT/OT-Geräte als Sprungbrett dienen, um tiefer in Netzwerke einzudringen und weiteren Schaden anzurichten. IoT/OT-Geräte können mit Ransomware infiziert werden, die wichtige Funktionen sperrt oder Daten verschlüsselt, bis ein Lösegeld bezahlt wird. Sie können auch in Botnetze eingebunden werden und dadurch eine Gefahr für andere Systeme darstellen.

- **Compliance-Verstösse**
  Unternehmen, die in regulierten Branchen tätig sind, könnten durch Sicherheitslücken in ihren IoT/OT-Systemen gegen Datenschutzgesetze oder Industriestandards verstossen, was zu Bussgeldern und Sanktionen führen kann. Der europäische Cyber Resilience Act wird besonders im Bereich der Produkthaftung zukünftig eine wichtige Rolle spielen. Die potenziellen Schäden und finanziellen Auswirkungen unsicherer IoT/OT-Geräte sind umfangreich und können ökonomische Verluste, Beeinträchtigung der öffentlichen Sicherheit, Unterbrechung kritischer Dienste und Verlust des öffentlichen Vertrauens umfassen. In extremen Fällen können Angriffe auf OT-Systeme in der kritischen Infrastruktur sogar zu Umweltkatastrophen oder Gefahren für das menschliche Leben führen.

Neben den direkten Kosten für die Behebung von Sicherheitsverletzungen und die Wiederherstellung betroffener Systeme müssen Unternehmen auch mit indirekten Kosten rechnen, wie z. B. Umsatzverlusten aufgrund von Betriebsunterbrechungen, Entschädigungszahlungen an betroffene Kunden oder Geschäftspartner und erhöhten Versicherungsprämien.

Die Herausforderung bei OT-Systemen besteht darin, dass

- diese z. T. über Service-Remotezugänge verfügen, welche über das Internet erreichbar sind;
- diese Systeme einerseits über sehr alte wie auch neue und komplexe Technologien verfügen und dass ebenso Legacy-Protokolle und -Geräte existieren, Security-Mechanismen (Verschlüsselung, Authentifizierung etc.) fehlen und einst getrennte Netze mit zunehmender Digitalisierung vernetzt werden;
- kaum noch Know-how-Träger und -Technik für den Support vorhanden sind (z. B. alte Windows-Versionen, Laptop mit RS232-Anschluss etc.);
- immer noch eine Diskrepanz zwischen Security und Safety und daraus abgeleitet eine unterschiedliche Zielsetzung, z. B. beim Zugriffsschutz durch Passwörter vs. Möglichkeit, im Gefahrenfall schnell eingreifen zu können, besteht;
- die Babyboomer-Generation, welche die Systeme kennt, in Pension geht;
- ein zunehmend regulativer Druck für Betreiber (NIS2, DORA etc.) und Hersteller (RED2, CRA etc.) festzustellen ist;
- die Wichtigkeit der Security in Organisationen verkannt wird oder unklare Zuständigkeiten bezüglich Security in den Organisationen bestehen.

Angesichts dieser Herausforderungen müssen Unternehmen proaktiv Massnahmen ergreifen, um ihre IoT- und OT-Geräte zu sichern. Dazu gehören:

- **Risikobewertung**
  Regelmässige Sicherheitsbewertungen und Audits, um potenzielle Schwachstellen zu identifizieren und zu beheben.

- **Sicherheitsrichtlinien**
  Es ist wichtig, Sicherheitsrichtlinien zu entwickeln und umzusetzen, die auf bewährten Standards wie der IEC-62443-Serie basieren. Diese Richtlinien ermöglichen eine sichere Konfiguration und Verwaltung von IoT/OT-Geräten. Darüber hinaus kann Security by Design bereits bei der Entwicklung der Geräte zu mehr Sicherheit beitragen.

- **Technologie aktuell halten**
  Veraltete Systeme aktualisieren und patchen, Vulnerability Management im Griff haben und gegebenenfalls das Netzwerk segmentieren.

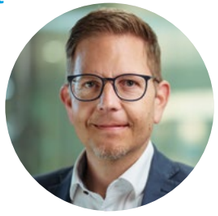
- **Schulung der Mitarbeitenden und der Servicetechniker**
  Sensibilisierung und Schulung der Mitarbeitenden im Umgang mit IoT/OT-Geräten, um menschliche Fehler zu minimieren.

- **Aktives Monitoring und Kontrollen**
  Regelmässige Sicherheitsüberprüfungen durchführen und Systeme kontinuierlich überwachen.

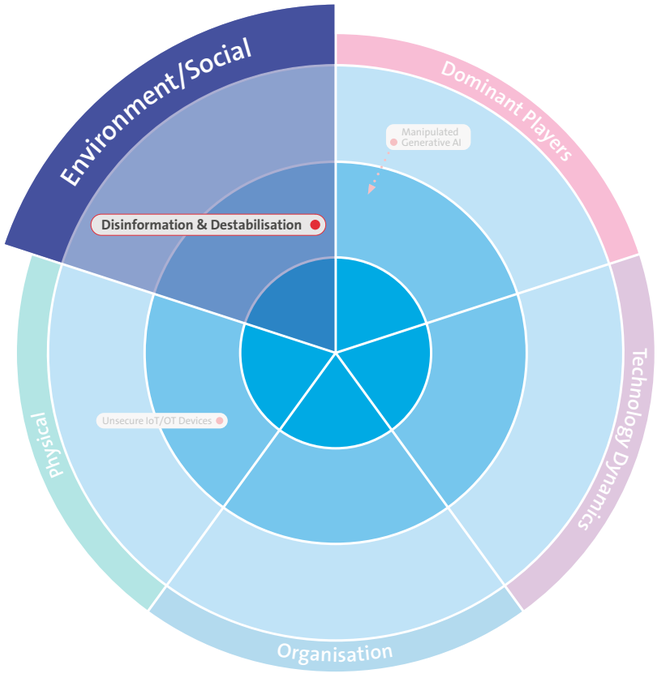
- **Zusammenarbeit mit vertrauenswürdigen Anbietern**
  Auswahl von Geräten und Software von Anbietern, die nachweislich Wert auf Sicherheit legen und regelmässige Updates bereitstellen.

« Die Sicherung der IoT- und OT-Infrastrukturen stellt für Unternehmen eine nicht zu unterschätzende Aufgabe dar, die von entscheidender Bedeutung für die Aufrechterhaltung der Betriebssicherheit und den langfristigen Geschäftserfolg ist. Die Sicherheit von OT-Systemen ist nicht optional und muss heute den gleichen Stellenwert wie die Sicherheit von IT-Systemen haben. »

Thomas Dummermuth
Head Physical Security & Safety, BCM



Disinformation & Destabilisation – Fakt ist?



Disinformation ist ein Thema, das in der heutigen Zeit für Unternehmen von grosser Bedeutung ist. Angesichts des exponentiellen Wachstums digitaler Plattformen und der Schnelligkeit, mit der Informationen verbreitet werden können, stehen Unternehmen vor der Herausforderung, die Integrität ihrer Informationen zu schützen und gleichzeitig gegen Falschinformationen vorzugehen, die ihre Marke, ihr Geschäft und ihre Sicherheitsvorgaben beeinträchtigen können.

Der Global Risks Report 2024 des World Economic Forum (WEF) hebt hervor, dass Disinformation eine gesellschaftliche Herausforderung und damit auch eine Bedrohung für Unternehmen und Organisationen darstellt. KI-generierte Fake News und Cyberangriffe seien weltweit das unmittelbare Top-Risiko – gerade mit Blick auf die anstehenden Wahlen in mehreren grossen Ländern wie den USA, Grossbritannien und Indien.

Auch Unternehmen sind zunehmend Ziel von Disinformation-Kampagnen, die beabsichtigen, ihr Ansehen zu schädigen, Verbraucher zu täuschen oder sogar den Börsenwert zu beeinflussen. In einer Ära, in der Informationen innerhalb von Sekunden global verbreitet werden können, ist die Fähigkeit eines Unternehmens, effektiv auf Disinformation zu reagieren, entscheidend für den Erhalt der Unternehmensintegrität und des Vertrauens der Stakeholder.

Die Risiken durch Disinformation umfassen nicht nur äussere Bedrohungen, wie die Beeinträchtigung der öffentlichen Wahrnehmung, sondern auch innere Risiken, wie die Verbreitung falscher Informationen innerhalb des Unternehmens, die zu Fehlentscheidungen und Sicherheitslücken führen können. Sicherheitsexperten unterstreichen, dass die Sicherheit von Unternehmensdaten und -infrastrukturen eng mit der Fähigkeit verbunden ist, Disinformation zu erkennen und zu bekämpfen. Gerade mit der rasanten Entwicklung von KI und der daraus folgenden Evolution von bild- und videogenerierenden KIs sind Deep-Fake-Angriffe und Disinformation-Kampagnen möglich, die mit herkömmlichen Mitteln nur schwer zu identifizieren sind.

Im Kontext der Cybersicherheit haben Disinformation-Kampagnen das Potenzial, nicht nur die öffentliche Meinung, sondern auch die internen Sicherheitsprotokolle von Unternehmen und Organisationen zu beeinträchtigen. Angreifer können Disinformation nutzen, um gezielte Phishing-Angriffe zu orchestrieren, Unsicherheit zu säen und Mitarbeitende dazu zu verleiten, vertrauliche Informationen preiszugeben oder schädliche Aktionen durchzuführen. Das Thema «Disinformation & Destabilisation» findet sich auch in den Angriffsvektoren «AI-Based Attacks» und «Big Data Analytics» wieder. Daher müssen die Identifikation und die Abwehr von Disinformation ein wichtiger Bestandteil der Sicherheitsvorgaben von Unternehmen sein.

Strategien für Unternehmen zum Umgang mit Disinformation

1. **Stärkung der internen Kommunikationskanäle:** Eine klare und transparente interne Kommunikationsstrategie ist essenziell, um sicherzustellen, dass Mitarbeitende richtige Informationen erhalten und verbreiten.

2. **Schulung und Sensibilisierung:** Mitarbeitende müssen regelmässig geschult werden, um Disinformation zu erkennen und richtig darauf zu reagieren. Dies beinhaltet das Verständnis der Risiken, die mit der Verbreitung falscher Informationen verbunden sind.

3. **Einsatz von Technologien:** Künstliche Intelligenz und maschinelles Lernen können Unternehmen dabei unterstützen, Disinformation-Kampagnen frühzeitig zu enttarnen. KI kann dabei helfen, die Verbreitung falscher Informationen zu analysieren, ihre Quellen zu identifizieren und entsprechende Gegenmassnahmen zu ergreifen.

4. **Proaktive Öffentlichkeitsarbeit und Krisenmanagement:** Im Falle einer Disinformation-Attacke ist eine schnelle und entschiedene Reaktion erforderlich. Unternehmen sollten Vorbereitungspläne entwickeln, um auf Disinformation reagieren zu können, einschliesslich der Zusammenarbeit mit Medien und der Nutzung eigener Kanäle, um korrekte Informationen zu verbreiten.

5. **Partnerschaften und Kooperationen:** Die Zusammenarbeit mit externen Experten, anderen Unternehmen und Organisationen kann wertvolle Einblicke in die besten Praktiken im Umgang mit Disinformation bieten und die Entwicklung gemeinsamer Standards und Reaktionen fördern.

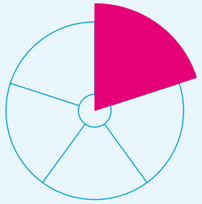
Unternehmen müssen Disinformation als ernsthafte Bedrohung für ihre Geschäftstätigkeit und ihren Ruf anerkennen. Die Allianz für Sicherheit in der Wirtschaft e. V. führte bereits 2019 in ihrer «Sicherheitsstudie zu Disinformation-Angriffen auf Unternehmen» den Disinformation-Schutz als vierten Quadranten in ihrem Sicherheitsfokus ein, und das aus gutem Grund.

Der WEF Global Risks Report 2024 verdeutlicht nochmal, dass die Bekämpfung von Disinformation eine entscheidende Komponente der Unternehmenssicherheit und der Unternehmensstrategie ist. Durch die Implementierung einer umfassenden Strategie, welche Aufklärung, Technologie und proaktives Engagement umfasst, können Unternehmen sich und ihre Stakeholder effektiv schützen. In einer Zeit, in der die Grenzen zwischen Wahrheit und falschen Informationen immer mehr verschwimmen, ist es entscheidend, dass Unternehmen an vorderster Front stehen, um die Integrität und die Vertrauenswürdigkeit ihrer Informationen zu bewahren.

« Die bewusste Verbreitung falscher Informationen, sogenannter Fake News, kann zu wirtschaftlicher und gesellschaftlicher Destabilisierung führen. Dafür wird gezielt auch der Cyberraum missbraucht. Unternehmen müssen sich dieser Gefahr bewusst sein, damit sie sich angemessen auf diese Art der Bedrohung vorbereiten und darauf reagieren können. »

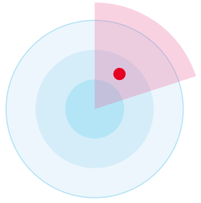
Marcus Beyer
Security Professional &
Security Awareness Officer

Details inkl. Tendenzen und Vergleich zum Vorjahr



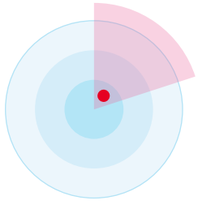
Dominant Players

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



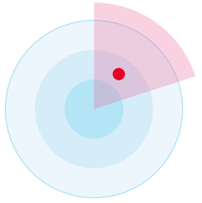
Concentration Data & Cloud Services
Die starke Zentralisierung von Daten in der Cloud führt zu Klumpenrisiken. Der Ausfall eines Service oder zentralen Dienstes kann weltweit Auswirkungen haben.

► Unverändert



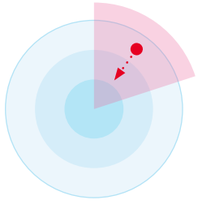
Infrastructure Integrity
In wesentliche Komponenten kritischer Infrastrukturen können fahrlässig oder bewusst Schwachstellen eingebaut worden sein, welche die Systemsicherheit gefährden.

► Unverändert



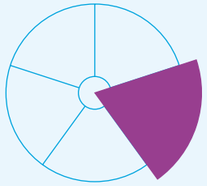
Legacy Protocols
Aufgrund von Softwareabhängigkeiten werden immer noch völlig veraltete, angreifbare Protokolle verwendet (z. B. NTLMv1, SMBv1, RC4), wodurch einige wenige Applikationen die Sicherheit ganzer Infrastrukturen gefährden.

► Unverändert



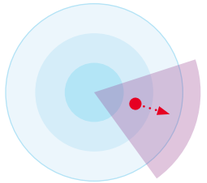
Manipulated Generative AI
Mit gezielten Manipulationen kann der Output eines KI-Systems verändert werden. Hier geht es um das Einschleusen von schlechten, falschen oder korrumpierten Daten bereits schon in der Trainingsphase, den Diebstahl von LL-Modellen, aber auch Prompt Manipulation, die zu unerwünschten und rechtlich bindenden Auswirkungen führen kann.

▲ Zunehmend



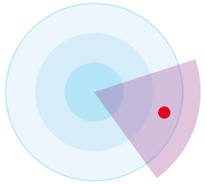
Technology Dynamics

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.



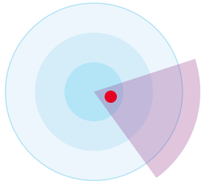
5G Security
5G ist eine noch junge Mobilfunktechnologie. Die Einführung wird neben vielen Chancen auch noch unbekannte Bedrohungen mit sich bringen.

▼ Abnehmend



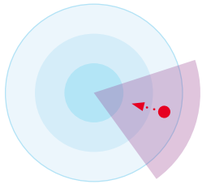
Quantum Computing
Quantencomputer können bestehende kryptografische Verfahren unbrauchbar machen, da sie diese in kürzester Zeit umgehen können.

► Unverändert



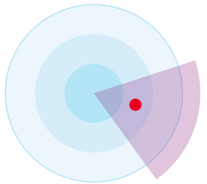
Ransomware
Kritische Daten werden grossflächig verschlüsselt und gegen Lösegeld (möglicherweise) wieder entschlüsselt.

► Unverändert



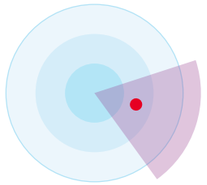
Increased Complexity
Die Komplexität von Systemen, insbesondere über Technologie- und Unternehmensgrenzen hinweg, nimmt laufend zu. Gerade im Hybrid-/Multi-Cloud-Umfeld mit vielen Cloud-Anbietern werden IT-Landschaften komplexer. Dadurch steigt die Risikoexposition und die Fehlersuche wird erschwert.

▲ Zunehmend



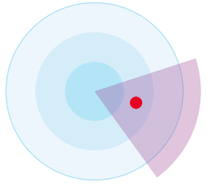
AI-Based Attacks
Angriffe mittels künstlicher Intelligenz (KI) sind gezielter und dadurch schwerer erkennbar. Durch KI können Angriffe effizienter auf klassische Angriffsvektoren wie z. B. Ransomware, Phishing, Spear-Phishing und vereinzelt auch auf neue Szenarien wie z. B. Deepfakes, Disinformation u. Ä. durchgeführt werden.

► Unverändert



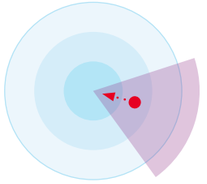
Targeted Attacks
Gezielte und komplexe Angriffe, um ein konkretes Ziel zu erreichen. Schlüsselpersonen werden identifiziert und gezielt direkt oder indirekt (Lateral Movement, Social-Engineering-Methoden) angegriffen, um dadurch relevante Informationen zu erhalten oder maximalen Schaden anzurichten.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

► Unverändert



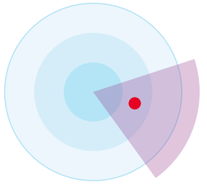
DDoS Attacks
Ein Distributed Denial-of-Service-(DDoS-)Angriff ist ein böswilliger Versuch, den normalen Datenverkehr eines Zielservers, -dienstes oder -netzwerks zu stören, indem das Ziel oder die umgebende Infrastruktur mit einer Flut von Internetverkehr überschwemmt wird. DDoS-Angriffe erreichen ihre 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



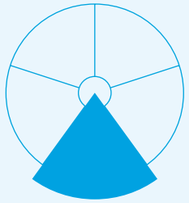
Supply Chain Attacks
Angriffe auf die Lieferkette zielen darauf ab, die Vertrauens- und Geschäftsbeziehungen zwischen einem Unternehmen und externen Parteien auszunutzen. Zu diesen Beziehungen können Partnerschaften, Lieferantenbeziehungen oder die Verwendung von Software Dritter gehören.

▲ Zunehmend



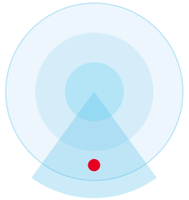
Subscriber Compromise
Schadsoftware verschafft sich Zugriff auf private Daten der Mobilnutzer oder wird für Angriffe auf die Telekommunikations- bzw. IT-Infrastruktur genutzt. Phishing, Smishing, Vishing und MFA-Bypass-Angriffe zielen auf die Subscriber Credentials. Durch die Folgeattacken werden so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

► Unverändert



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, z. B. «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 heran an die Business Units 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

Digitalisation
Immer stärkere Vernetzung der realen mit der virtuellen Welt im Privat- und im Geschäftsleben führt zu mehr Angriffswegen. Auch das neue «New Work» und das Verschieben der Arbeit in Homeoffice-Umgebungen erhöhen das Cyberrisiko und die Angreifbarkeit der IT-Infrastruktur über ungesicherte Endgeräte.

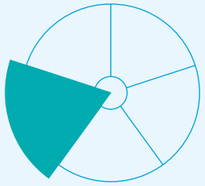
► Unverändert

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

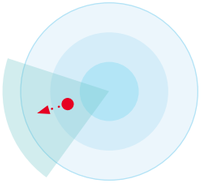
Infrastructure Misconfiguration
Ausnutzung von fehlkonfigurierten Infrastrukturkomponenten und/oder von Schwachstellen, die spät identifiziert und behoben werden. Bei einer stärkeren Automatisierung technischer Betriebsprozesse wird dies bei erfolgreichen Angriffen oder Fehlkonfigurationen grössere Auswirkungen haben.

- Unverändert



Physical

Unter diesen Begriff fallen Angriffe auf die Infrastruktur im Cyberspace, die vermehrt Schaden in der physischen Welt verursachen werden. 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) o. Ä. sind wichtige Punkte. Den Medien ist zu entnehmen, dass die Verwundbarkeit kritischer Infrastrukturen durch Cyberangriffe stark zugenommen hat.

▼ Abnehmend

Targeted Sabotage
Es geht um die gezielten Attacken auf wichtige kritische Infrastrukturen, Versorgungsanlagen und Leitungen, was zu beachtlichen Einschränkungen im Internet führen kann. 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.

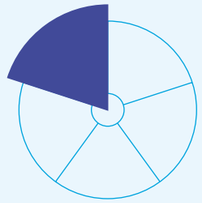
► Unverändert

Unsecure IoT/OT Devices
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. der Verfügbarkeit oder Datenintegrität, eingeschränkt werden.

► Unverändert

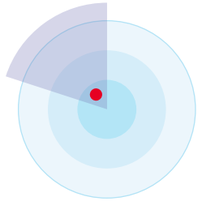
Environmental Influence
Durch die Klimakrise treten vermehrt unvorhersehbare Wetterphänomene und Wettereinflüsse wie Hitze, Starkregen, Tornados, Hagel, Blitzintensitäten u. Ä. auf, welche Schäden an der Infrastruktur von Organisationen und Unternehmen verursachen können und damit eine hohe Auswirkung auf die externe und die interne Umgebung eines Informationssystems oder Netzwerks haben.

► Unverändert



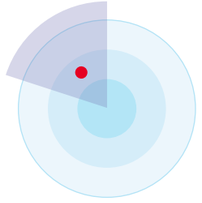
Environment/Social

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



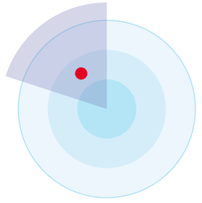
Security Job Market
Der Bedarf an Security Professionals ist enorm gross und kann nur sehr schwer gedeckt werden. Dies führt zu einem abnehmenden Know-how im Kampf gegen immer komplexere und intelligentere Angriffe.

► Unverändert



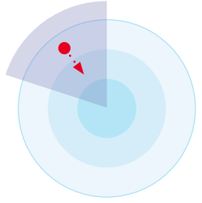
Digital Identity
Beglaubigte, persönliche digitale Identitäten können missbraucht oder gestohlen werden, um z. B. unter fremdem Namen Verträge abzuschliessen.

► Unverändert



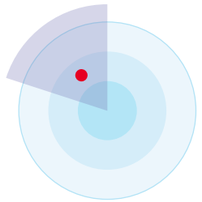
Disinformation & Destabilisation
Die absichtliche Verbreitung von unwahren Informationen kann zu einer wirtschaftlichen und gesellschaftlichen Destabilisierung führen und wird gerade in Krisenzeiten vermehrt auch über den Cyberraum gezielt eingesetzt.

► Unverändert



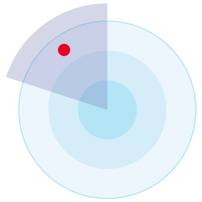
Political Influence
Politische Strömungen können Einfluss auf technologische oder wirtschaftliche Entscheide nehmen, z. B. bei der Auswahl von Technologielieferanten. Daraus können neue Risiken entstehen.

▲ Zunehmend



Big Data Analytics
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 Disinformation, Fake News, gesellschaftliche und psychosoziale Analysen sowie die Erstellung von Bewegungsmustern herangezogen. Mit Letzterem geht eine Verletzung der Privatsphäre einher.

- Unverändert



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 Gruppen von Hacktivisten, staatlichen Akteuren und organisierter Kriminalität, welche durch Auftragsarbeiten zunehmend Druck auf Unternehmen und Organisationen ausüben. Auch Kollateralschäden durch Hack-Back-Strategien einzelner Länder wird hier vermehrt Beachtung geschenkt.

- Unverändert

Fazit

Eine starke Cyberresilienz kann nur interdisziplinär und abteilungsübergreifend realisiert werden. Dabei hilft das folgende 5-Schritte-Modell:

1. **Identify**
   Die Identifikation beinhaltet die Analyse der vorhandenen Daten, deren Schutzrelevanz sowie die Speicherung und die Verarbeitung dieser Daten. Ebenfalls wichtig sind das Wissen über potenzielle Risiken und Bedrohungen sowie die Gewährleistung des Schutzes in der Lieferkette.

2. **Protect**
   Mitarbeitende auf allen Hierarchieebenen müssen im Thema Cybersicherheit geschult und sensibilisiert werden. Auch Bug-Bounty-Programme und Red-Teaming-Angriffe helfen, die Resilienz zu stärken. Des Weiteren ist es ratsam, neue Sicherheitsphilosophien wie Zero Trust zu integrieren.

3. **Detect**
   Das kontinuierliche Überwachen der eigenen Infrastruktur und des internen Netzwerks ist essenziell. Auch eine stärkere Automatisierung des Security Operations Center ist sinnvoll.

4. **Respond**
   Es ist enorm wichtig, bei Sicherheitsvorfällen schnell zu reagieren. Ebenso sollten auch «Near Misses» erkannt und dokumentiert werden, um daraus zu lernen. Zudem sollte auch ein einsatzfähiges Krisenmanagement aufgebaut und trainiert werden.

5. **Recover**
   Eine gut vorbereitete Kommunikationsstrategie für den Krisenfall hilft, das Vertrauen zu halten. Auch Service- und Business-Continuity-Pläne sind zu empfehlen, um den reibungslosen Betrieb sicherzustellen.

Die physische Sicherheit darf nicht vernachlässigt werden, auch wenn sie in der Cybersicherheit oft zu kurz kommt. Physische Angriffe können die Widerstandsfähigkeit (Resilienz) von Unternehmen gegenüber Cyberbedrohungen gefährden.

Beispielsweise können extreme Wettereinflüsse wie Dürre, Hitze, Überschwemmungen und Kälteperioden zu Schäden an der Infrastruktur führen, die sich auf die Stabilität der Cyberservices auswirken können, sowohl auf nationaler wie auch auf internationaler Ebene. Umgekehrt können auch Cybervorfälle schwerwiegende Auswirkungen auf physische Bereiche haben. Daher ist es wichtig, sowohl die physische als auch die cyberbezogene Sicherheit zu berücksichtigen und angemessene Massnahmen zu ergreifen, um die Resilienz von Unternehmen zu gewährleisten.

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)
Copyright	© April 2024 by Swisscom (Schweiz) AG, Group Security, Alte Tiefenaustrasse 6, 3048 Worblaufen, swisscom.ch
Druck	OK DIGITALDRUCK AG, Zürich
Auflage	200 Exemplare

Als «Innovator of Trust» ermöglicht und gestaltet Swisscom die digitale Zukunft. Mit innovativen Produkten und Services und dem Vertrauen der Kundschaft wird ein einzigartiges Kundenerlebnis mit nachhaltigem Einfluss auf Umwelt und Gesellschaft geschaffen. In der Schweiz und in der ganzen Welt.

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

Du suchst bei Swisscom einen Job im Security-Bereich? Dann schau hier und bewirb dich: swisscom.ch/securityjobs

#BeTheStrongestLink