swisscom

Cybersecurity Threat Radar 2025

Cyberresilienz trotz geopolitischer Herausforderungen

Inhalt

Cybersecurity Threat Radar

Cyberresilienz trotz geopolitischer Herausforderungen

Für Unternehmen ist es in der sich schnell wandelnden Welt der Cybersicherheit unerlässlich, ihre Abwehrstrategien kontinuierlich zu überprüfen und anzupassen. Cyberkriminelle werden immer raffinierter und ändern ihre Angriffsmethoden stetig. Dies macht aufseiten der Verteidigung innovative und flexible Lösungsansätze erforderlich. Im vorliegenden Cybersecurity Threat Radar geben wir Ihnen einen Einblick in die aktuellen Schwerpunkte und Herausforderungen im Bereich der Cyberresilienz, mit denen wir uns bei Swisscom intensiv auseinandersetzen.

Im Kampf gegen konkrete Cyberbedrohungen legen wir unsere Priorität auf die gezielte Weiterentwicklung unserer Detection & Response Capabilities. Die Basis dafür bilden die praktischen Erkenntnisse aus Red-Team-Übungen, Incident-Response-Erfahrungen und aktuellen Threat-Intelligence-Informationen.

Auch die Bedeutung grundlegender Sicherheitspraktiken, oft als «Cyberhygiene» bezeichnet, kann nicht genug betont werden. Diese Basics bilden das Fundament einer robusten Cybersicherheitsstrategie und sind entscheidend für die erfolgreiche Abwehr einer Vielzahl von Bedrohungen. Wir legen grossen Wert auf die Implementierung und kontinuierliche Verbesserung dieser grundlegenden Sicherheitsmassnahmen. Dazu gehören auch regelmässige Sicherheitsupdates, starke Authentifizierungsmethoden und regelmässige Schulung unserer Mitarbeitenden zur Förderung des allgemeinen Sicherheitsbewusstseins.

Die sich verändernde geopolitische Lage stellt Unternehmen im Bereich der Cybersicherheit vor neue Herausforderungen. Der wachsende Einfluss von Techmilliardären, politische Verschiebungen in Europa und strengere Regulierungen erfordern eine flexible und vorausschauende Sicherheitsstrategie.

Um diesen Herausforderungen zu begegnen, setzen wir bei Swisscom auch gezielt auf eine enge Zusammenarbeit mit nationalen und internationalen Partnern. Unser Computer Security Incident Response Team (CSIRT) tauscht sich regelmässig mit anderen Betreibern kritischer Infrastrukturen und Sicherheitsdienstleistern aus, um ein umfassendes Bild der aktuellen Bedrohungslage zu erhalten.

Blicken wir in die Zukunft, sehen wir uns mit neuen technologischen Entwicklungen konfrontiert, die sowohl Chancen als auch Risiken bergen. So erfordert beispielsweise der Einsatz von generativer KI in der Cybersicherheit einen ausgewogenen Ansatz: Einerseits nutzen wir diese Technologie zur Verbesserung unserer Bedrohungserkennung, andererseits müssen wir uns gegen ihre missbräuchliche Verwendung durch Cyberkriminelle wappnen.

Darüber hinaus gewinnt das Konzept der «Zero-Trust»-Architektur zunehmend an Bedeutung. Es stellt inhärentes Vertrauen innerhalb der IT-Infrastruktur konsequent infrage und prüft jeden einzelnen Zugriff. Damit erhöhen Unternehmen nicht nur ihre Sicherheit, sondern treiben auch die digitale Transformation voran.

Zusammenfassend kann gesagt werden, dass die Stärkung der Cyberresilienz ein kontinuierlicher Prozess ist, der Wachsamkeit, Anpassungsfähigkeit und auch Innovationskraft erfordert. Bei Swisscom versuchen wir auf einen ganzheitlichen Ansatz zu setzen, der reale Bedrohungen, grundlegende Sicherheitspraktiken und zukunftsweisende Technologien gleichermassen berücksichtigt. Nur so können wir den vielfältigen Cyberbedrohungen effektiv begegnen und die digitale Zukunft unserer Kunden und Partner sicher gestalten.

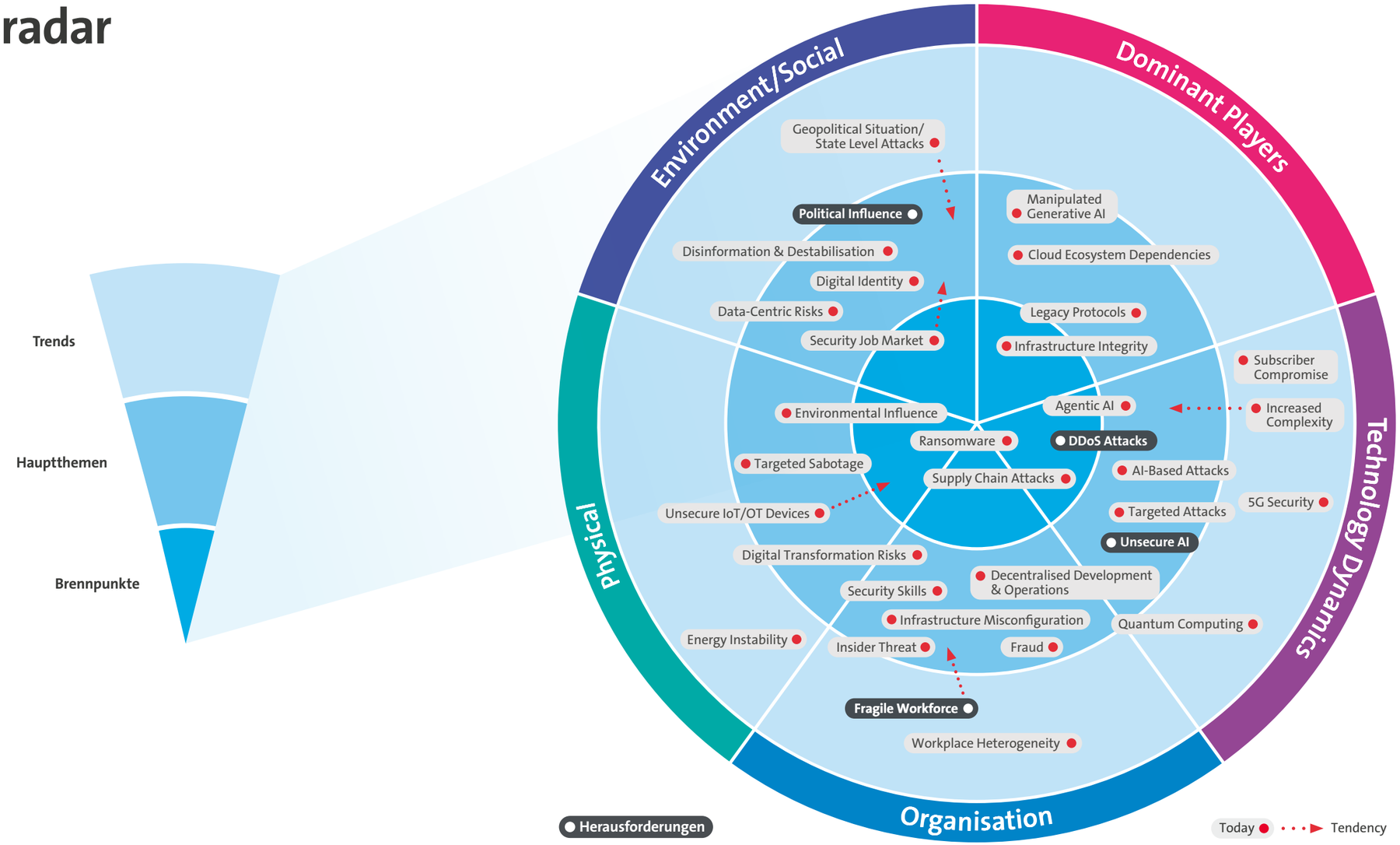
« Die sich verändernde geopolitische Lage stellt Unternehmen im Bereich der Cybersicherheit vor neue Herausforderungen. Der wachsende Einfluss von Techmilliardären, politische Verschiebungen in Europa und strengere Regulierungen erfordern eine flexible und vorausschauende Sicherheitsstrategie. »

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.



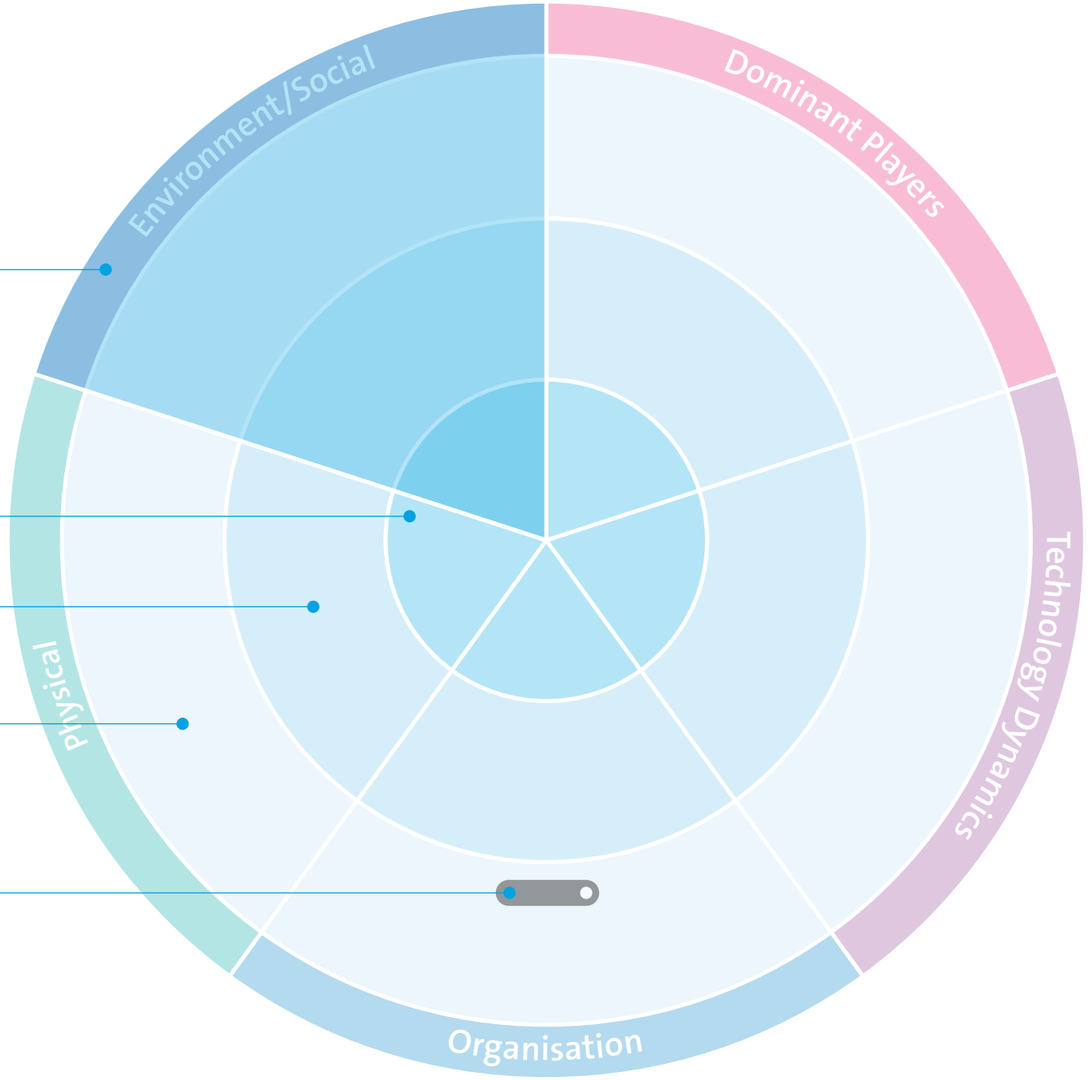
Methodik

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.

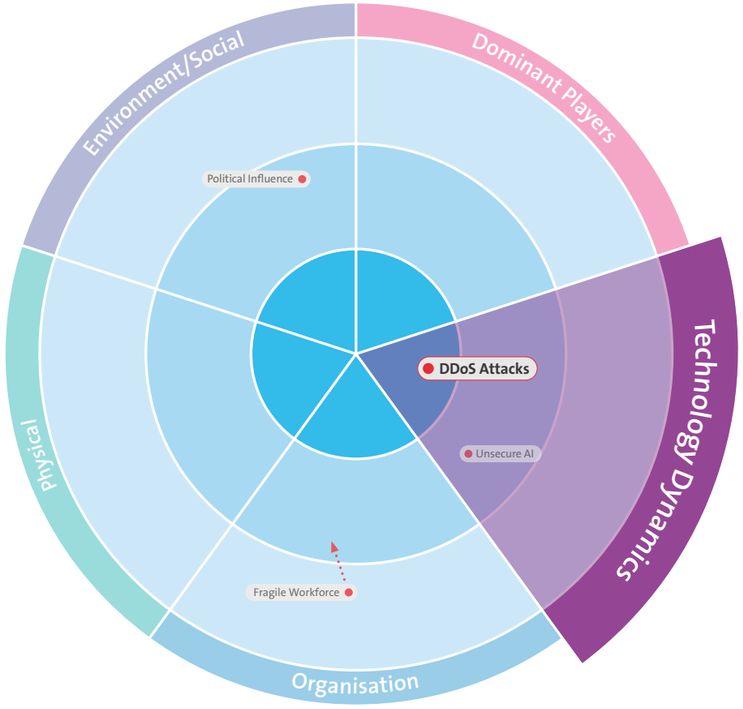
Die Kreise kennzeichnen wir als:

- **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.



DDoS Attacks: «Macht kaputt, was euch kaputt macht»



In einer zunehmend digitalisierten Geschäftswelt stellen DDoS-Attacken (Distributed Denial of Service) eine ernsthafte und wachsende Bedrohung für Unternehmen dar. Diese Angriffe zielen darauf ab, Onlinedienste, Websites oder Netzwerke durch eine Flut von Datenverkehr unzugänglich zu machen, was weitreichende Folgen für betroffene Unternehmen haben kann. Die DDoS-Attacke gegen Swisscom im August 2024 schaffte es sogar in die Medien.

Die Anzahl gezielter DDoS[1]-Attacken auf Finanzdienstleister, die öffentliche Verwaltung, Hostinganbieter, Energieanbieter, Telekommunikationsanbieter, Onlineshops u.a. hat sich in der Schweiz von 2023 auf 2024 verdoppelt. Gemäss dem NETSCOUT Cyber Threat Horizon Report wurden 2023 56 200 und 2024 rund 107 000 DDoS-Attacken unterschiedlichster Art registriert. Pro Tag fanden im vergangenen Jahr 293 Attacken statt. Auch die Schweizer Telekommunikationsbranche wurde ins Visier der Angreifer genommen.

Bedrohungsszenario

Das Ausführen von DDoS-Attacken wird immer einfacher. Im Internet werden auf kriminellen Marktplätzen seit Jahren DDoS-Attacken gegen eine geringe Gebühr (ab 15 USD pro Monat) als Dienstleistung angeboten, «Cybercrime as a Service» gewissermassen – oder als Stresstest. Diese Angebote nehmen zu. Es ist also damit zu rechnen, dass die Anzahl der DDoS-Angriffe weiter steigen wird.

Dazu kommt, dass es für Cyberkriminelle dank des Siegeszugs der künstlichen Intelligenz (KI) immer einfacher wird, ihre DDoS-Attacken gefährlicher und wirkungsvoller zu gestalten.

Für das Risikomanagement rückt damit der Schutz von immateriellen Vermögenswerten wie Daten, Netzwerken oder geistigem Eigentum in den Vordergrund. Unzureichende IT-Sicherheit muss als Unternehmensrisiko eingestuft werden, wenn durch Cyberattacken ganze Betriebe lahmgelegt werden können.

[1] DDoS (Distributed Denial of Service) ist eine Art von Cyberangriff, bei dem öffentlich erreichbare IP-Adressen aus dem Internet gezielt mit einer sehr grossen Anzahl von Anfragen von infizierten PCs, TV-Geräten, Webcams und vielen anderen IP-Geräten geflutet werden. Das Ziel der Angreifer ist es, die e-Services, die über die attackierten IP-Adressen erreichbar sind, möglichst lange offline zu setzen.

Warum sind DDoS-Attacken gefährlich für Unternehmen?

1. **Betriebsunterbrechungen:** DDoS-Angriffe können den normalen Geschäftsbetrieb erheblich stören, indem sie Websites, Onlinedienste oder interne Netzwerke lahmlegen.
2. **Finanzielle Verluste:** Unternehmen, insbesondere solche mit starker Abhängigkeit vom Onlineverkehr, können erhebliche Umsatzeinbussen erleiden, wenn ihre Dienste nicht verfügbar sind.
3. **Reputationsschaden:** Wiederholte oder lang anhaltende Ausfälle können das Vertrauen der Kunden in die Zuverlässigkeit und Sicherheit des Unternehmens untergraben.
4. **Hohe Wiederherstellungskosten:** Die Kosten für die Wiederherstellung der Dienste und die Verstärkung der Sicherheitsinfrastruktur nach einem Angriff können beträchtlich sein.
5. **Ablenkungsmanöver:** DDoS-Attacken können als Ablenkung dienen, um von anderen bösartigen Aktivitäten, wie beispielsweise Datendiebstahl, abzulenken.

Schadenspotenzial

Ein finanzieller Schaden kann für ein Unternehmen bereits auftreten, bevor es zu einer DDoS-Attacke kommt. Das Bundesamt für Cybersicherheit (BACS) berichtet von Erpressungsversuchen im Internet, bei denen Unternehmen gedroht wird, sie über DDoS anzugreifen, sollten sie nicht bereit sein, die geforderte Summe zu bezahlen. Nicht immer haben die Erpresser tatsächlich die Fähigkeit, eine DDoS-Attacke auszuführen. Aber sie pokern und hoffen darauf, dass alleine die Drohung für eine Lösegeldzahlung genügt.

Schutzmassnahmen

DDoS-Attacken stellen eine ernsthafte und wachsende Bedrohung für Unternehmen aller Grössenordnungen dar. Mit der zunehmenden Digitalisierung und der steigenden Abhängigkeit von Onlinediensten wird die Bedeutung robuster Schutzmassnahmen weiter zunehmen. Unternehmen müssen proaktiv handeln, um ihre digitale Infrastruktur zu schützen und so die Kontinuität ihres Geschäftsbetriebs zu gewährleisten. Wie in anderen Bereichen gilt: «Vorsorge ist besser als Nachsorge.»

« Chancen und Risiken sind permanente Begleiter im Internet. Beide Parameter können Sie bewusst beeinflussen. Zuwarten und hoffen, nie Opfer einer DDoS-Attacke zu werden, ist definitiv nicht zu empfehlen. Treffen Sie gezielte Massnahmen und setzen Sie diese schnellstmöglich um. »

Beat Hunziker
Senior Product Manager Business Internet & Security Services

Die Investitionen in umfassende DDoS-Schutzlösungen, kontinuierliche Schulungen und die Entwicklung flexibler Reaktionspläne sind entscheidend, um den Herausforderungen der sich ständig weiterentwickelnden Cyberlandschaft zu begegnen. Nur durch eine ganzheitliche und vorausschauende Herangehensweise können Unternehmen ihre Widerstandsfähigkeit gegen DDoS-Angriffe stärken und potenzielle Schäden minimieren.

Letztendlich ist der Schutz vor DDoS-Attacken nicht nur eine technische Herausforderung, sondern eine strategische Notwendigkeit für jedes moderne Unternehmen. Die Fähigkeit, solche Angriffe effektiv abzuwehren, wird zunehmend zu einem entscheidenden Wettbewerbsvorteil in der digitalen Wirtschaft.

« Die Bedrohung von DDoS-Angriffen ist allgegenwärtig. Sie verursachen nicht nur finanzielle Schäden, sondern können auch den Ruf eines Unternehmens empfindlich treffen. »

Reto Friedl
Product Manager Managed Security Services

Fragile Workforce: «Wenn der Druck zu stark wird»

Cybersecurity-Teams stehen unter enormem Druck. Die Bedrohungslandschaft verändert sich ständig – von hochentwickelten Phishingangriffen über gezielte Ransomware-Attacken bis hin zu Deepfake-Manipulationen. Gleichzeitig wächst die Komplexität der IT-Infrastrukturen, während Angriffsflächen durch hybride Arbeitsmodelle und vernetzte Geräte zunehmen.

Mehr als 10 000 Warnmeldungen am Tag: Warum ist das problematisch?

Warnmeldungen, Incident-Analysen und sich rasch wandelnde Bedrohungsszenarien führen zu «Alert Fatigue» – einem Zustand, in dem Warnsignale nicht mehr mit der nötigen Aufmerksamkeit verfolgt werden, weil das System überlastet ist. Eine Studie von Devo Technology zeigt, dass 42 % der IT-Security-Teams regelmässig Alarme ignorieren, weil sie zu zahlreich und unübersichtlich sind. Unachtsamkeit und Fehlentscheidungen sind die Folge, was ein erhebliches Sicherheitsrisiko darstellt.

Herausforderung: Die kognitive und emotionale Belastung managen

Diese Herausforderungen haben gravierende Folgen für die Mitarbeitenden: Chronischer Stress beeinträchtigt nicht nur die Gesundheit, sondern auch die Arbeitsleistung. Eine aktuelle Branchenstudie von SoSafe zeigt, dass bis zu 57 % der Sicherheitsprofis im DACH-Raum unter Burn-out leiden. Die Hauptgründe sind:

- **Hoher Leistungsdruck:** Ständige Bedrohungserkennung und Abwehr als Kernaufgabe.
- **Überlastung und Überstunden:** Regelmässige Arbeitszeiten werden überschritten.
- **Unzureichende Schulung:** Fehlende Weiterbildung führt zu Unsicherheit.
- **Personalmangel:** Fehlende Fachkräfte erhöhen die Belastung zusätzlich.

Zusätzlich entsteht ein «Cognitive Overload», eine mentale Überlastung, wenn das Gehirn mit zu vielen Informationen, Aufgaben und Entscheidungen gleichzeitig kämpfen muss. Ablenkungen, Multitasking und ständiger Stress verschärfen das Problem – sichere Entscheidungen werden dadurch immer schwieriger. Typische Folgen sind:

- Verzögerte Reaktionen auf Bedrohungen
- Fehlkonfigurationen und Sicherheitslücken
- Eingeschränkte Kommunikation unter Stress
- Burn-out und hohe Fluktuation

Die Konsequenz: Wer mentale Belastung ignoriert, riskiert nicht nur die Sicherheit des Unternehmens, sondern auch die Gesundheit der Menschen, die sie schützen.

Strategien für sicheres, effektives und gesundes Arbeiten

Ein nachhaltiger Ansatz adressiert diese Kernbereiche: Führung, Teamdynamik und Schlüsselkompetenzen.

Führungskräfte als Firewall gegen Überlastung

Führungskräfte spielen eine zentrale Rolle dabei, achtsames Arbeiten vorzuleben, regelmässige Gespräche zu führen und mentale Gesundheit als Priorität zu setzen. Sie helfen, Strukturen für fokussiertes Arbeiten zu schaffen und unnötige Unterbrechungen zu minimieren. Gleichzeitig können sie durch präventive Massnahmen psychologische Sicherheit fördern und Überlastung verhindern.

Auch HR-Verantwortliche sollten aktiv werden, indem sie z.B. betriebliches Gesundheitsmanagement fördern. So entsteht eine Unternehmenskultur, in der psychische Stabilität als Erfolgsfaktor gilt.

Psychologische Sicherheit als Grundlage für effektive Teamarbeit
Ein resilientes Cybersecurity-Team braucht psychologische Sicherheit. Wissen teilen, offen über Fehler sprechen und in Stresssituationen kollegial unterstützen stärkt die Widerstandsfähigkeit des Teams. Erfolgsfaktoren dabei sind:

- **Emotionale Intelligenz fördern –** bewusste Wahrnehmung und Unterstützung innerhalb des Teams.
- **Mentoring-Programme etablieren –** Erfahrungsaustausch und individuelle Entwicklung.
- **Peer-Gruppen nutzen –** Best Practices und psychische Herausforderungen reflektieren.

Schlüsselkompetenzen für resiliente Cybersecurity-Teams
Eine mentale Agilität ist trainierbar – und wer sie beherrscht, reduziert nicht nur Fehler, sondern auch Stress. Die Fähigkeit, schnell auf Bedrohungen zu reagieren und gleichzeitig durchdachte Entscheidungen zu treffen, ist essenziell:

- Mentale Agilität ermöglicht den flexiblen Wechsel zwischen analytischem Denken und schnellem Handeln.
- Mentale Klarheit stellt sicher, dass unter Druck relevante Informationen bewertet werden, statt impulsiv zu reagieren.

Warum hilft das gegen Stress?
Cybersecurity-Profis müssen trainieren, bewusst zwischen den Denksystemen zu wechseln, um Fehlentscheidungen zu vermeiden. Unter hohem Druck oder bei kognitiver Überlastung übernimmt oft das intuitive, schnelle, aber fehleranfällige Denken – ein Konzept, das Psychologe Daniel Kahneman als «System 1» beschreibt. Das reflektierte, analytische «System 2» hilft dagegen, präzisere Entscheidungen zu treffen, benötigt aber mehr kognitive Ressourcen.

- Wer bewusst zwischen System 1 und 2 wechseln kann, trifft sicherere Entscheidungen und reduziert Stress.
- Gezielte Steuerung der Denksysteme verhindert impulsive Reaktionen und erhöht die Kontrollfähigkeit in kritischen Situationen.
- Weniger kognitive Überlastung verringert mentalen Druck und verbessert langfristig die Widerstandskraft gegenüber Stress.

« Slight Destroyers: Wer sie ignoriert, riskiert die Sicherheit. »

Anja Peter
CEO & Co-Founder Human Empowerment Center AG

Fokussierung und Regeneration
Dauerhaft im Krisenmodus zu arbeiten, ist mental und körperlich nicht nachhaltig. Wer ständig zwischen Aufgaben springt und ohne Pausen arbeitet, erschöpft seine kognitiven Ressourcen. Studien zeigen, dass permanente Reizüberflutung durch Multitasking und ständige Unterbrechungen die Fähigkeit zur Fokussierung und Problemlösung drastisch reduzieren. Gezielte Regeneration steigert die langfristige Widerstandskraft. Dazu gehören:

- **Deep Work und Time-Blocking –** gezielte Phasen ungestörten Arbeitens, um kognitive Ressourcen effizient zu nutzen.
- **Fokus-Sprints –** intensive Arbeitsphasen mit klar definierten Pausen, um mentale Ermüdung zu vermeiden.
- **Mikroauszeiten und Atemtechniken –** gezielte Entlastung des Nervensystems, um Konzentration und Stressbewältigung zu verbessern.

Wer bewusst zwischen Fokus und Erholung wechselt, schützt seine mentale Leistungsfähigkeit. Achtsames Arbeiten bedeutet, sich nicht von Ablenkungen steuern zu lassen, sondern gezielt zu entscheiden, worauf man seine Aufmerksamkeit richtet. Ohne diese bewusste Steuerung bleibt das Gehirn im ständigen Alarmmodus, was langfristig zu Erschöpfung und Fehlentscheidungen führt.

Fazit: Nachhaltige Cybersecurity beginnt mit resilienten Teams
Ein resilientes Security-Team ist entscheidend für den Erfolg in der Cybersecurity. Dauerhafte Spitzenleistungen erfordern Resilienz und Unterstützung für die Menschen hinter den Monitoren.

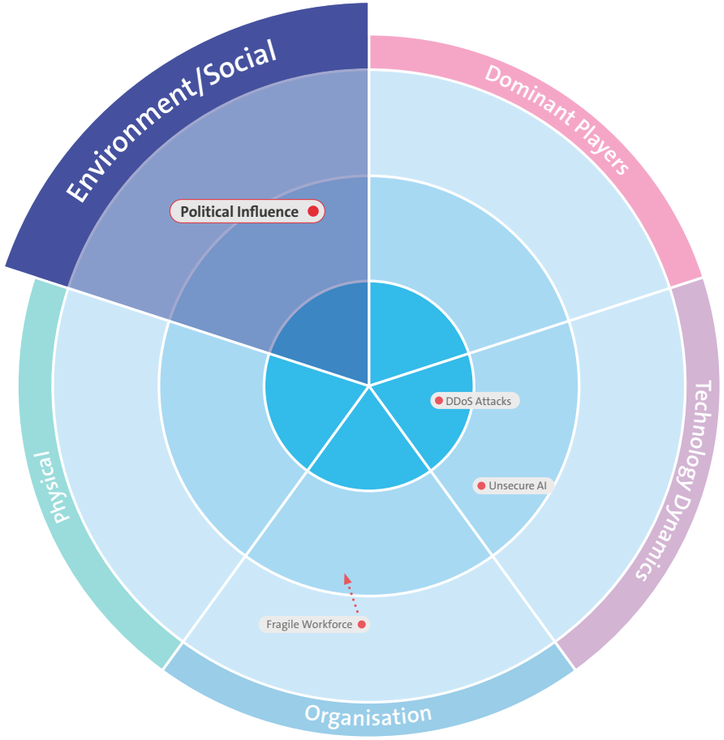
Ziel muss es sein, ein Umfeld zu schaffen, in dem Achtsamkeit, psychologische Sicherheit und aktives Stressmanagement selbstverständlich sind. Nur so lassen sich Cognitive Overload, Alert Fatigue sowie die viel zitierten «slight destroyers of strong cybersecurity» entschärfen. Auf diese Weise gewinnt das Unternehmen oder die Organisation nicht nur motivierte und gesunde Mitarbeitende, sondern erhöht langfristig auch die gesamte Widerstandsfähigkeit gegenüber Cyberangriffen. Nur so kann eine starke und widerstandsfähige Workforce aufgebaut werden, die den Herausforderungen der Zukunft gewachsen ist.

Letztlich steht und fällt jede Sicherheitsstrategie mit den Menschen, die sie umsetzen. Eine resiliente Workforce ist der Schlüssel zu einer widerstandsfähigen Cybersecurity – für Unternehmen und die Gesundheit derjenigen, die sie schützen.

« Eine fragile Workforce reagiert, eine resiliente Workforce agiert. »

Martina Novo
Tribe Chief Security

Political Influence: «Mehr Sicherheit durch mehr Vorgaben?»



Wir befinden uns in einer Epoche tiefgreifender Umbrüche, in der geopolitische, wirtschaftliche und technologische Entwicklungen für allgemeine Verunsicherung sorgen können. Dieser Trend wird als «Age of Disorder» oder auch «Zeitalter der Störung» bezeichnet. In diesen Zeiten braucht es Verlässlichkeit, Stabilität und Führung. Unternehmen und der Staat stehen unter erheblichem Druck, da hybride Bedrohungen, wie gezielte Desinformation, Cyberangriffe und Sabotageakte, darauf abzielen, das Vertrauen in politische Institutionen zu untergraben, gesellschaftliche Ängste zu schüren und den sozialen Zusammenhalt zu schwächen.

Unternehmen und Staaten müssen sich also auf eine nachhaltige und digitale Transformation fokussieren, um wirtschaftliche Stabilität gewährleisten zu können. Resilienzstrategien, wie Diversifizierung und Cybersicherheit, sind essenziell, um zukünftige Krisen abzufedern. Das «Zeitalter der Störung» erfordert vorausschauendes Handeln, um disruptive Veränderungen zu antizipieren und aktiv zu gestalten. Nur wer agil Innovationen vorantreibt und mutig den Wandel mitgestaltet, kann sich im globalen Wettbewerb behaupten.

Die digitale Transformation bietet nicht nur Herausforderungen, sondern auch zahlreiche Chancen. Unternehmen, die in der Lage sind, sich schnell an neue Gegebenheiten anzupassen und innovative Lösungen zu entwickeln, werden im globalen Wettbewerb erfolgreich sein. Dies erfordert jedoch eine Kultur der Offenheit und des kontinuierlichen Lernens, in der Fehler als Lernmöglichkeiten betrachtet und neue Ideen gefördert werden.

In diesem, sich rasant entwickelnden Umfeld, stehen Unternehmen vor der Herausforderung, Cybersicherheit zu gewährleisten und gleichzeitig innovativ zu bleiben. Regulierungen wie z.B. NIS2, DORA, der Cyber Resilience Act (CRA), Standards wie ISO 27001 oder auch nationale Vorgaben wie das Informationssicherheitsgesetz (ISG) in der Schweiz sollen dabei helfen.

Doch die zunehmende Regulierungsdichte birgt auch Risiken eines sogenannten «Regulierungsparadoxes»: Unternehmen und Organisationen wähnen sich in einer scheinbaren Sicherheit und konzentrieren sich darauf, regulatorische Anforderungen abzuhaken, anstatt ganzheitlich über das Thema Sicherheit nachzudenken.

Um diesem Trend entgegenzuwirken, müssen Unternehmen ein Gleichgewicht zwischen Compliance und proaktivem Sicherheitsmanagement finden und einen risikoorientierten Ansatz verfolgen, der den Fokus auf tatsächliche Bedrohungen anstelle blosser Vorschrifteneinhaltung legt. Regelmässige Überprüfungen der Sicherheitslage über regulatorische Anforderungen hinaus sind notwendig, um flexibel auf neue Bedrohungen reagieren zu können. Es ist entscheidend, dass Organisationen die Eigenverantwortung für ihre Sicherheit wahrnehmen und nicht ausschliesslich auf externe Vorgaben setzen. Nur durch eine Kombination aus regulatorischer Einhaltung, einem starken und selbst gesteuerten Sicherheitsmanagement sowie einer nachhaltigen und wirksamen Sicherheitskultur können Unternehmen resilient gegen Cyberbedrohungen werden.

In einer Welt, die sich ständig verändert, ist es unerlässlich, dass Unternehmen und Staaten nicht nur auf aktuelle Bedrohungen reagieren, sondern auch proaktiv Massnahmen ergreifen, um zukünftige Herausforderungen zu bewältigen. Eine kontinuierliche Anpassung und Verbesserung der Sicherheitsstrategien sowie eine enge Zusammenarbeit zwischen verschiedenen Akteuren als auch ein Verständnis für die Sachlage sind dabei unerlässlich. Nur durch gemeinsame Anstrengungen können wir eine sichere und stabile digitale Zukunft gestalten.

Die Resilienz und die Verfügbarkeit von Diensten und Infrastrukturen sind ebenfalls von zentraler Bedeutung. Unternehmen müssen sicherstellen, dass ihre Systeme auch in Krisenzeiten funktionsfähig bleiben und schnell wiederhergestellt werden können. Hier benötigt es eine enge Zusammenarbeit zwischen verschiedenen Abteilungen und eine klare Kommunikation über die Verantwortlichkeiten und Massnahmen im Falle eines Vorfalls.

Die Kontrolle über digitale Schlüsselprozesse und die sie befähigenden Infrastrukturen ist entscheidend, um die digitale Souveränität zu gewährleisten. Unternehmen müssen sicherstellen, dass sie die Kontrolle über ihre Daten und Systeme behalten und nicht von externen Anbietern abhängig sind. Dies erfordert eine sorgfältige Planung und Umsetzung von Sicherheitsmassnahmen sowie eine kontinuierliche Überwachung und Anpassung an neue Bedrohungen. Unternehmen müssen sicherstellen, dass ihre Systeme und Daten vor unbefugtem Zugriff geschützt sind und dass sie in der Lage sind, auf Sicherheitsvorfälle schnell und effektiv zu reagieren.

Digitale Souveränität

Der Zugang zu vertrauenswürdigen Informationen ist ein weiterer wichtiger Aspekt der digitalen Souveränität. Unternehmen und Regierungen müssen sicherstellen, dass sie über verlässliche und aktuelle Informationen verfügen, um fundierte Entscheidungen treffen zu können. Dies erfordert eine enge Zusammenarbeit mit verschiedenen Informationsquellen und die Fähigkeit, Informationen schnell und effizient zu verarbeiten und zu analysieren.

« Gesellschaftspolitik und Innovation verändern unsere Welt rasanter denn je. Doch Zukunft passiert nicht – sie wird von denen gemacht, die mit Resilienz, Agilität und Weitsicht vorangehen. »

Florian Kässberger
Experience Innovation Expert

Insgesamt ist es entscheidend, dass Unternehmen und Staaten einen ganzheitlichen Ansatz verfolgen, um die Herausforderungen der digitalen Transformation zu bewältigen. Dies erfordert eine enge Zusammenarbeit zwischen verschiedenen Akteuren, eine kontinuierliche Anpassung und Verbesserung der Sicherheitsstrategien sowie eine Kultur der Offenheit und des kontinuierlichen Lernens. Nur durch gemeinsame Anstrengungen können wir eine sichere und stabile digitale Zukunft gestalten.

Cybersicherheit ist und bleibt ein zentraler Bestandteil der digitalen Souveränität von Unternehmen und Organisationen, d.h.

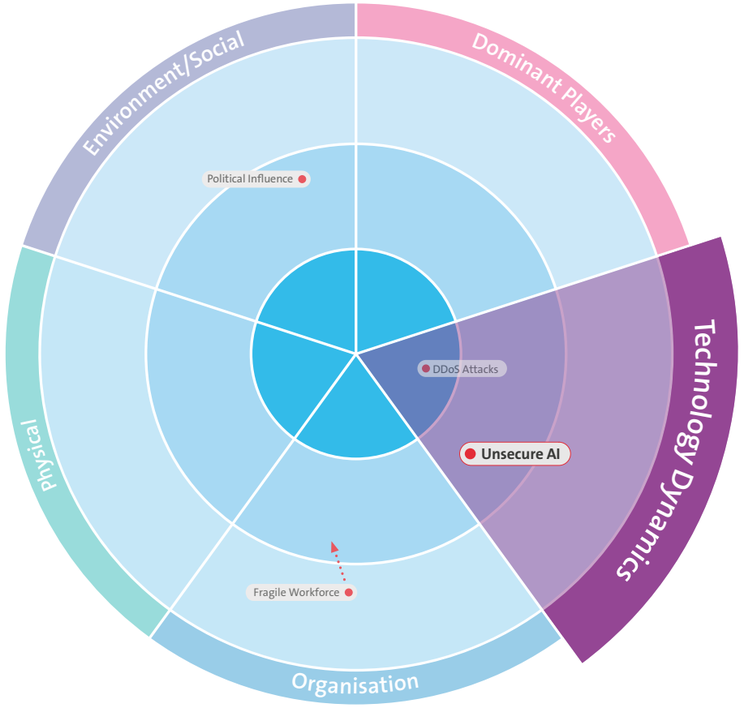
- Resilienz und Verfügbarkeit von Diensten und Infrastrukturen
- Kontrolle über Daten und Datenflüsse
- Kontrolle über digitale Schlüsselprozesse sowie der sie befähigenden Infrastrukturen und Organisationen
- Zugang zu vertrauenswürdigen Informationen
- Cybersicherheit
- Digitale Kompetenzen
- Diversifizierte Lieferketten

Und wir alle sind gefordert, unseren Beitrag zur digitalen Souveränität zu leisten. Die Wirtschaft ist bereit, den Dialog zu führen und ihren Beitrag zu leisten. Gerade für die Machbarkeit und Umsetzung der digitalen Souveränität ist die Stimme der Branche wichtig.

« Digitale Souveränität ist kein Endziel, sondern ein laufender Prozess und erfordert eine ganzheitliche Betrachtung. »

Karin Stöckli
Public Affairs Delegate of
Federal Administration and NGO

Shadow AI: «Gekommen, um zu bleiben – KI um jeden Preis?»



In der heutigen schnelllebigen Wirtschaft setzen Unternehmen vermehrt auf künstliche Intelligenz (KI), um wettbewerbsfähig zu bleiben. Doch neben den offiziell implementierten KI-Systemen gibt es ein weniger bekanntes Phänomen: **Shadow AI.**

Schatten-KI betrifft Unternehmen aller Grössen und Branchen. Ähnlich wie Shadow IT bezieht sich das Phänomen «Shadow AI» auf die Nutzung von KI-Tools und -Anwendungen innerhalb eines Unternehmens, die ohne Genehmigung der IT oder des Sicherheitsteams erfolgt. Dies kann harmlos erscheinen, birgt jedoch erhebliche Risiken. Laut einer Studie von Gartner nutzen über 50 % der Mitarbeiter KI oder Machine-Learning-Anwendungen für ihre Arbeit, von denen die IT-Abteilung keine Kenntnis hat. Dies kann unter Umständen zu schwerwiegenden Vorfällen führen wie:

- Datenschutzverletzungen und Sicherheitsrisiken.
- Compliance-Verstösse, insbesondere im Bereich Daten- und Geheimhaltungsschutz oder auch im Hinblick auf den EU AI Act (sofern für Unternehmen in der Schweiz anwendbar).
- Ineffizienzen durch doppelte Ausgaben und inkonsistente Prozesse.
- Potenzielle Reputationsschäden bei Bekanntwerden von Missbrauch.

Der EU AI Act ist ein Gesetz der EU, kann unter bestimmten Bedingungen aber auch für Unternehmen in der Schweiz relevant sein. Der AI Act wird zusätzliche Anforderungen an Unternehmen stellen:

- Risikobasierte Kategorisierung von KI-Systemen. Je höher das Risiko, desto strengere Anforderungen.
- Kontrollen für Hochrisiko-KI-Anwendungen.
- Transparenzpflichten für bestimmte KI-Systeme.
- Hohe Strafen bei Nichteinhaltung (je nach Verstoss bis zu 30 Millionen Euro oder 6 % des weltweiten Jahresumsatzes).

Erscheinungsformen der Schatten-AI

- **KI-betriebene Chatbots:** Diese werden oft ohne Genehmigung zur Bearbeitung von Kundenanfragen eingesetzt, was zu ungenauen Antworten führen kann.
- **Machine-Learning-Modelle:** Mitarbeiter nutzen externe Plattformen zur Datenanalyse, was vertrauliche Daten gefährden kann.
- **Marketing-Automatisierungstools:** Diese steigern zwar die Produktivität, können aber Compliance-Regeln verletzen und das Kundenvertrauen schädigen.
- **AI-Funktionalität in Unternehmenssoftware:** Eine zusätzliche AI-Funktionalität wird nach einem Update einer bestehenden Applikation ohne zusätzliche Prüfung aktiviert und gibt unberechtigten Personen sensitive Daten preis.

Chancen und Herausforderungen

Die Integration von KI in Unternehmensprozesse bietet enormes Innovationspotenzial. KI kann dazu beitragen, Geschäftsprozesse zu optimieren, neue Produkte und Dienstleistungen zu entwickeln und die Kundenzufriedenheit zu erhöhen. Durch die Analyse grosser Datenmengen können Unternehmen wertvolle Einblicke gewinnen und fundierte Entscheidungen treffen. KI-gestützte Automatisierung kann die Effizienz steigern und Mitarbeiter von repetitiven Aufgaben entlasten, sodass sie sich auf strategische Tätigkeiten konzentrieren können.

Künstliche Intelligenz ist aus unserer heutigen Arbeitswelt nicht mehr wegzudenken, dient als Innovationstreiber und kann – richtig angewendet – die Produktivität steigern. Allerdings müssen Unternehmen die Risiken durch klare Richtlinien und Überwachung minimieren.

Um die Herausforderungen der Schatten-AI zu meistern, ist es entscheidend, dass Unternehmen eine Kultur der Transparenz und Zusammenarbeit zwischen IT und Fachabteilungen fördern. Durch regelmässige Audits und Schulungen können potenzielle Risiken frühzeitig erkannt und behoben werden. Nur so kann die Schatten-AI in ein kontrolliertes und sicheres KI-Ökosystem integriert werden.

«Jedes Unternehmen, das KI-Tools einsetzt, sollte künftig eine unternehmensweite AI Governance aufbauen – dies nicht nur, um Reputationsrisiken vorzubeugen, sondern auch, um bestehenden und künftigen Regulierungen gerecht zu werden. Die KI-Technologie entwickelt sich rasch weiter, weshalb es umso wichtiger ist, Schritt zu halten und einen verantwortungsvollen Einsatz sicherzustellen.»

Anne-Sophie Morand
Data Governance Counsel

Massnahmen zur Integration von Schatten-KI und Innovation durch AI

Um Schatten-KI zu adressieren und sich auf den EU AI Act vorzubereiten, sollten Unternehmen folgende Massnahmen ergreifen:

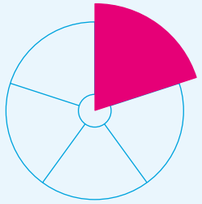
- **Bestandsaufnahme und Risikobewertung:** Identifizieren Sie alle KI-Systeme im Unternehmen und bewerten Sie deren Risiken mit Blick auf die einschlägigen Gesetzesbestimmungen (z.B. Datenschutzrecht oder EU AI Act, sofern anwendbar).
- **Governance und Richtlinien:** Entwickeln Sie klare KI-Nutzungsrichtlinien und etablieren Sie einen Genehmigungsprozess für neue KI-Tools.
- **Technische Kontrollen:** Implementieren Sie Netzwerküberwachung und DLP-Systeme.
- **Schulung und Sensibilisierung:** Führen Sie regelmässige AI-spezifische Mitarbeiterschulungen durch und fördern Sie eine offene Kommunikationskultur zu KI-Themen.
- **Bereitstellung genehmigter KI-Lösungen:** Evaluieren und stellen Sie offizielle KI-Tools bereit.
- **Compliance-Management:** Richten Sie ein KI-Ethik-Komitee ein und implementieren Sie Prozesse zur kontinuierlichen Überwachung und Dokumentation.
- **Zusammenarbeit und Expertise:** Etablieren Sie ein KI-Kompetenzzentrum und arbeiten Sie eng mit Rechts- und Compliance-Experten zusammen.

Durch diese Massnahmen können Unternehmen Schatten-KI effektiv managen und gleichzeitig den gesetzlichen Anforderungen gerecht werden. Es ist wichtig, einen proaktiven Ansatz zu verfolgen, um sowohl die Chancen der KI zu nutzen als auch die damit verbundenen Risiken zu minimieren.

«Datenschutzverletzungen und Sicherheitsrisiken sind bei der Nutzung von KI-Tools noch viel zu wenig im Fokus von Nutzenden und Unternehmen. Zusätzlich zu den Chancen von KI in Kombination mit der Verarbeitung von grossen Datenmengen birgt gerade dies potenziell erhebliche Risiken.»

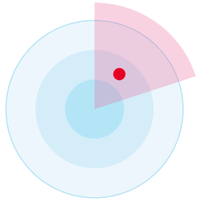
Marc Scheidegger
Solution Security Architect für Data, Analytics & AI

Details inkl. Tendenzen und Vergleich zum Vorjahr



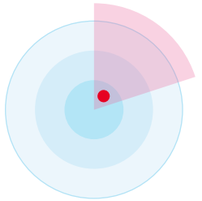
Dominant Players

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



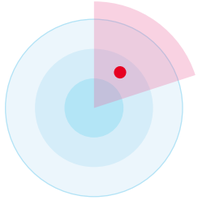
Cloud Ecosystem Dependencies
Die starke Zentralisierung von Daten in der Cloud führt zu Klumpenrisiken. Der Ausfall eines Service oder zentralen Dienstes kann weltweit Auswirkungen haben.

- Unverändert



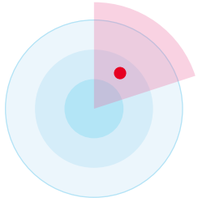
Infrastructure Integrity
In wesentliche Komponenten kritischer Infrastrukturen können fahrlässig oder bewusst Schwachstellen eingebaut worden sein, welche die Systemsicherheit gefährden.

- Unverändert



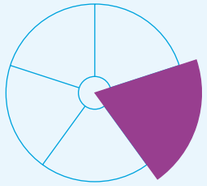
Legacy Protocols
Aufgrund von Softwareabhängigkeiten werden immer noch völlig veraltete, angreifbare Protokolle verwendet (z.B. NTLMv1, SMBv1, RC4), wodurch einige wenige Applikationen die Sicherheit ganzer Infrastrukturen gefährden.

- Unverändert



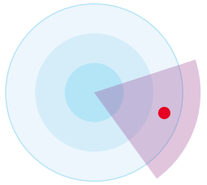
Manipulated Generative AI
Mit gezielten Manipulationen kann der Output eines KI-Systems verändert werden. Hier geht es um das Einschleusen von schlechten, falschen oder korrumpierten Daten bereits schon in der Trainingsphase, den Diebstahl von LL-Modellen, aber auch Prompt Manipulation, die zu unerwünschten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

- Unverändert



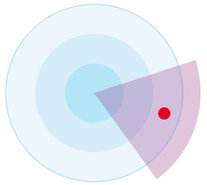
Technology Dynamics

Unter diesem Begriff sind Bedrohungen zu verstehen, die von der rasanten technologischen Innovation ausgehen und 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.



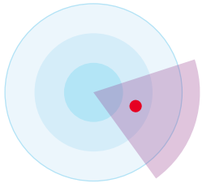
5G Security
5G ist eine noch junge Mobilfunktechnologie. Die Einführung wird neben vielen Chancen auch noch unbekannte Bedrohungen mit sich bringen.

► Unverändert



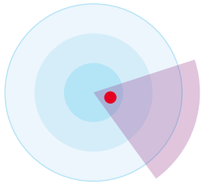
Quantum Computing
Quantencomputer können bestehende kryptografische Verfahren unbrauchbar machen, da sie diese in kürzester Zeit umgehen können.

► Unverändert



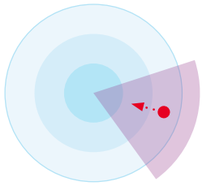
Unsecure AI
Unsichere KI-Systeme gefährden Lieferketten und den Datenschutz, da generative Modelle vertrauliche Daten unkontrolliert offenlegen können. Dadurch kann nicht nur die Geschäftskontinuität beeinträchtigt, sondern auch der Ruf eines Unternehmens erheblich geschädigt werden. Zudem drohen regulatorische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

► Unverändert



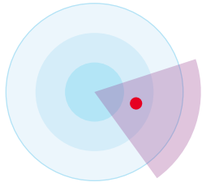
Ransomware
Kritische Daten werden grossflächig verschlüsselt und gegen Lösegeld (möglicherweise) wieder entschlüsselt.

► Unverändert



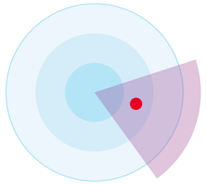
Increased Complexity
Die Komplexität von Systemen, insbesondere über Technologie- und Unternehmensgrenzen hinweg, nimmt laufend zu. Gerade im Hybrid-/Multi-Cloud-Umfeld mit vielen Cloud-Anbietern werden IT-Landschaften komplexer. Dadurch steigt die Risikoexposition und die Fehlersuche wird erschwert.

▲ Zunehmend



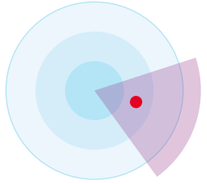
AI-Based Attacks
Angriffe mittels künstlicher Intelligenz (KI) sind gezielter und dadurch schwerer erkennbar. Durch KI können Angriffe effizienter auf klassische Angriffsvektoren wie z.B. Ransomware, Phishing, Spear-Phishing und vereinzelt auch auf neue Szenarien wie z.B. Deepfakes, Desinformation u.Ä.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

► Unverändert



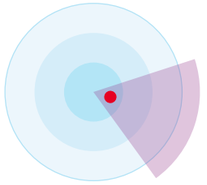
Agentic AI
Agentic-KI ist proaktiv und in der Lage, eigenständig Entscheidungen zu treffen und Strategien anzupassen. Dadurch erhöht sich die Angriffsfläche, da selbstlernende und adaptive Systeme unvorhersehbare Verhaltensweisen entwickeln und eigenständig Interaktionen mit Umsystemen durchführen können. 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 ein scheinbar harmloser Copilot kann durch fehlerhafte Anweisungen oder Manipulation seitens der Angreifer erheblichen Schaden verursachen.

► Unverändert



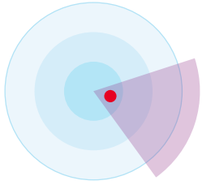
Targeted Attacks
Gezielte und komplexe Angriffe, um ein konkretes Ziel zu erreichen. Schlüsselpersonen werden identifiziert und gezielt direkt oder indirekt (Lateral Movement, Social-Engineering-Methoden) angegriffen, um relevante Informationen zu erhalten oder maximalen Schaden anzurichten. Ein wesentlicher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

► Unverändert



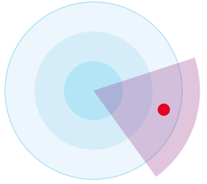
DDoS Attacks
Ein Distributed-Denial-of-Service (DDoS)-Angriff ist ein böswilliger Versuch, den normalen Datenverkehr eines Zielservers, -dienstes oder -netzwerks zu stören, indem das Ziel oder die umgebende Infrastruktur mit einer Flut von Internetverkehr überschwemmt wird. DDoS-Angriffe erreichen ihre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



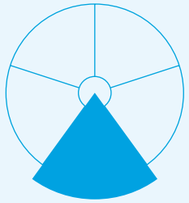
Supply Chain Attacks
Angriffe auf die Lieferkette zielen auf die Ausnutzung von Vertrauens- und Geschäftsbeziehungen zwischen einem Unternehmen und externen Parteien ab. Zu diesen Beziehungen können Partnerschaften, Lieferantenbeziehungen oder die Verwendung von Software Dritter gehören.

► Unverändert



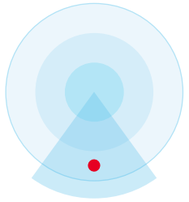
Subscriber Compromise
Schadsoftware verschafft sich Zugriff auf private Daten der Mobilnutzer oder wird für Angriffe auf die Telekommunikations- bzw. IT-Infrastruktur genutzt. Phishing, Smishing, Vishing und MFA-Bypass-Angriffe zielen auf die Subscriber Credentials. Durch die Folgeattacken werden so 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, wie 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 an die Business Units bei gleichzeitig kürzer werdenden Release-Zyklen heran. Dadurch wird die Kontrolle/Steuerung der Sicherheit erschwert.

► Unverändert

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

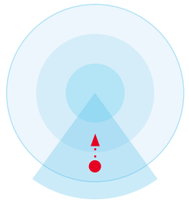
► Unverändert

Digital Transformation Risks
Immer stärkere Vernetzung der realen und 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



Fragile Workforce
Eine fragile Arbeitsorganisation beschreibt die Anfälligkeit von Cybersecurity- und Cyber-Defense-Teams für psychische Belastungen und 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.

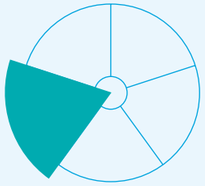
▲ Zunehmend

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

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

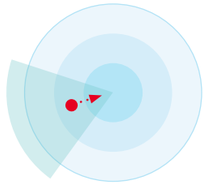
Unter diesen Begriff fallen Angriffe auf die Infrastruktur im Cyberspace, die vermehrt Schaden in der physischen Welt verursachen werden. Aber auch Bedrohungen, die von der physischen Umgebung ausgehen und in der Regel eher auf physische Ziele ausgerichtet sind, zählen dazu.

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.

► Unverändert

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

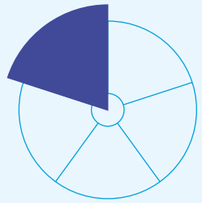


Unsecure IoT/OT Devices
Ob Betriebstechnologie (OT) zur Überwachung und Steuerung von physischen Prozessen, Geräten und Infrastrukturen oder IoT Geräte – das Internet der Dinge ist immer und überall. Dabei werden hier verschiedenste Aufgaben – von simpel bis komplex – erfüllt, die von Home-Entertainment-Anwendungen, der 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.

▲ Zunehmend

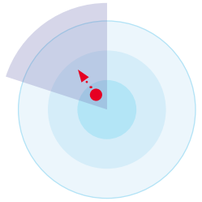
Environmental Influence
Durch die Klimakrise treten vermehrt unvorhersehbare Wetterphänomene und Wettereinflüsse wie Hitze, Starkregen, Tornados, Hagel, Blitzintensitäten u.Ä. auf, welche Schäden an der Infrastruktur von Organisationen und Unternehmen verursachen können und damit eine hohe Auswirkung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

► Unverändert



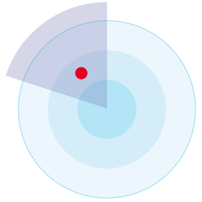
Environment/Social

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



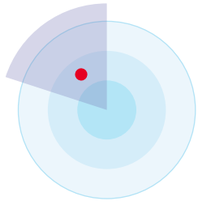
Security Job Market
Der Bedarf an Security Professionals ist enorm gross und kann nur sehr schwer gedeckt werden. Dies führt zu einem abnehmenden Know-how im Kampf gegen immer komplexere und intelligentere Angriffe.

▼ Abnehmend



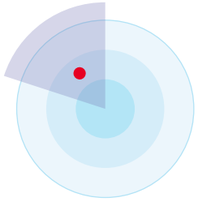
Digital Identity
Beglaubigte, persönliche digitale Identitäten können missbraucht oder gestohlen werden, um z.B. unter fremdem Namen Verträge abzuschliessen.

► Unverändert



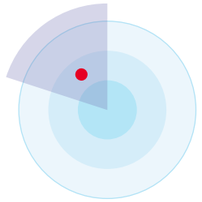
Disinformation & Destabilisation
Die absichtliche Verbreitung von unwahren Informationen kann zu einer wirtschaftlichen und gesellschaftlichen Destabilisierung führen und wird gerade in Krisenzeiten vermehrt auch über den Cyberraum gezielt eingesetzt.

► Unverändert



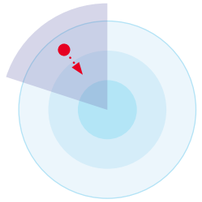
Political Influence
Politische Strömungen, aber auch Regularien und Vorgaben können Einfluss auf technologische oder wirtschaftliche Entscheide nehmen, z.B. bei der Auswahl von Technologielieferanten. Daraus können neue Risiken entstehen.

► Unverändert



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 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 zunehmend Druck auf Unternehmen und Organisationen durch Auftragsarbeiten ausüben. Auch Kollateralschäden durch Hack-Back-Strategien einzelner Länder wird hier vermehrt Beachtung geschenkt.

▲ Zunehmend

Fazit

Die digitale Transformation stellt Unternehmen und Institutionen vor zahlreiche Herausforderungen.

Auch die geopolitische Situation, mit der wir uns tagtäglich auseinandersetzen müssen, hat einen direkten Einfluss auf technologische und wirtschaftliche Entscheidungen. Dazu zählen etwa der Umgang mit unkontrollierten KI-Anwendungen, die Gewährleistung der allgemeinen Cybersicherheit und der Schutz der Cybersecurity-Teams vor Überlastung. Unternehmen sind deshalb gut beraten, Resilienzstrategien zu entwickeln, um disruptive Veränderungen zu antizipieren und sich im globalen Wettbewerb erfolgreich behaupten zu können. Ein gesundes Gleichgewicht zwischen Compliance und proaktivem Sicherheitsmanagement zu finden, ist dabei entscheidend. Eine nachhaltige Arbeitsweise erfordert eine Kultur der Transparenz, psychologische Sicherheit und kontinuierliche Weiterbildung. Führungskräfte spielen eine zentrale Rolle dabei, mentale Überlastung zu verhindern und eine resiliente Arbeitsumgebung zu schaffen.

Deshalb sollten Unternehmen und Institutionen in dieser sich rasant entwickelnden digitalen Welt proaktiv handeln, um die Chancen der digitalen Transformation zu nutzen und die damit verbundenen Risiken gleichzeitig aktiv zu minimieren. Dies erfordert eine enge Zusammenarbeit zwischen verschiedenen Akteuren, eine kontinuierliche Überprüfung und Verbesserung der Sicherheitsstrategien sowie eine Kultur der Offenheit und des kontinuierlichen Lernens.

Wer in Unternehmen und Organisationen auf innovative Lösungen setzt, fördert eine transparente und sicherheitsbewusste Unternehmenskultur und investiert in die kontinuierliche Weiterbildung der Teams. So kann eine sichere digitale Zukunft geschaffen werden, damit Unternehmen, Organisationen und Staaten resilient gegen Sicherheitsbedrohungen werden. Wir alle können dabei mithelfen und mit gutem Vorbild vorangehen. Lassen Sie uns gemeinsam die Chancen der digitalen Zukunft nutzen.

#BeTheStrongestLink

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 2025 by Swisscom (Schweiz) AG, Group Security, Alte Tiefenaustrasse 6, 3048 Worblaufen, swisscom.ch
Druck	OK DIGITALDRUCK AG, Zürich
Auflage	140 Exemplare

Als «Innovator of Trust» ermöglicht und gestaltet Swisscom die digitale Zukunft. Mit innovativen Produkten und Services und dem Vertrauen der Kunden 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

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

#BeTheStrongestLink