swisscom

Cyber Security Threat Radar
2021/2022

Risiken und Umfeld stets neu bewerten

Inhalt

«Nur eine genau an die Bedürfnisse der Anwender angepasste Security wird mittel- und langfristig ihrer Aufgabe gerecht werden und die notwendige Resilienz schaffen.»

Cyber Security Threat Radar

Was bis vor Kurzem noch undenkbar war, ist seit dem 24. Februar traurige Realität. **Der Krieg in Europa verändert gerade unsere Welt.**

Mir wurden mit dem Ausbruch des Krieges in der Ukraine die Rolle und Wichtigkeit der (sozialen) Medien nochmals in aller Deutlichkeit bewusst. Aufwühlende Berichte, krasse Falschmeldungen und virtuose Auftritte wechseln sich permanent mit subtiler Desinformation ab.

Fakt ist: Viele Bedrohungen und Risiken sind mit Beginn der russischen Invasion in der Ukraine noch stärker in den Fokus von Regierungen, Organisationen und Unternehmen gerückt, als es schon in der pandemischen Situation in den letzten zwei Jahren der Fall gewesen war. Die angespannte Situation macht sich in der gesamten Gesellschaft bemerkbar.

Die gute Nachricht: Trotz der schwierigen Lage konnte in der Schweizer Netzinfrastruktur bislang keine Zunahme der Angriffe beobachtet werden.

Natürlich versuchen Cyberkriminelle, den Ukraine-Krieg für ihre illegalen Machenschaften zu missbrauchen, beispielsweise über entsprechend adaptierte Phishing-Versuche oder manipulierte Spendenaufrufe. Dies ist aber bei Grossereignissen leider Usus. Die Anzahl der illegalen Cyberaktivitäten bleibt also auf konstant hohem Niveau, nur die Story dahinter wurde angepasst.

Ich hoffe, der vorliegende Cyber Security Threat Radar 2021/2022 liefert Ihnen wertvolle Insights zum Thema Cybersicherheit und unterstützt Sie beim Ausbau Ihrer Aktivitäten rund um das Thema Sicherheit in Ihrem Unternehmen oder Ihrer Organisation.

Philippe Vuilleumier
Head of Group Security
Swisscom (Schweiz) AG

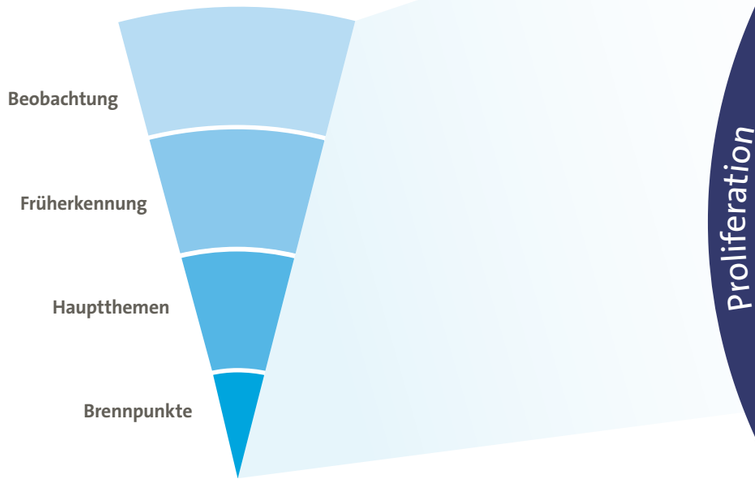
Meine Aussage aus dem letztjährigen Cyber Security Threat Radar: «Besondere Lagen erfordern besondere Massnahmen im Umfeld von Sicherheit, Schutz und Risikobewusstsein» hat an Relevanz nichts eingebüsst – im Gegenteil. Gerade in dieser disruptiven Lage ist es wichtig, den Überblick zu behalten, um zeitgerecht die richtigen Massnahmen treffen zu können.

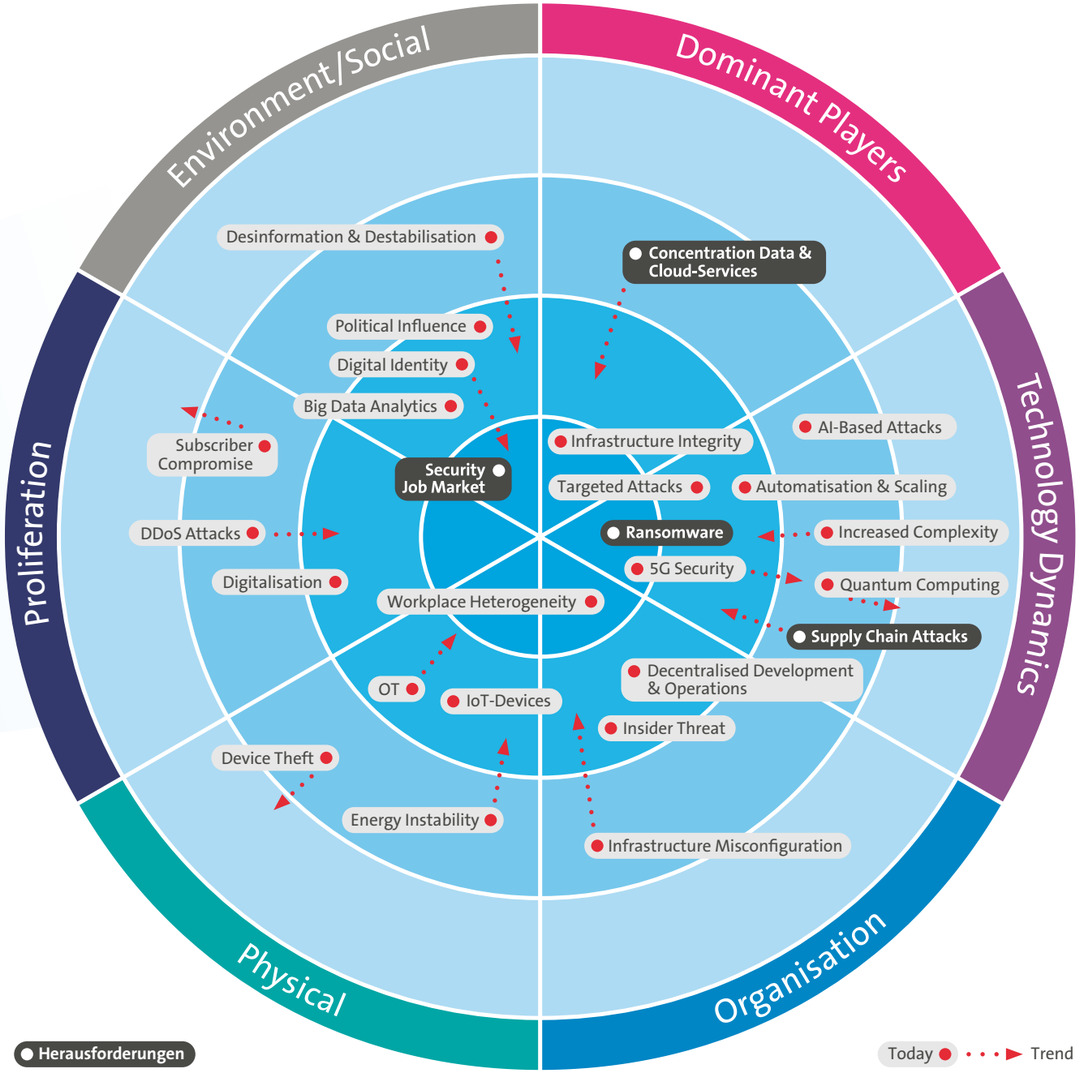
Im Zentrum dieser Massnahmen steht der Mensch. Selbstverständlich bilden Technologien unersetzliche Bausteine des Sicherheitsdispositivs. Doch sie allein garantieren keinen Schutz. Deshalb empfehle ich dringend, bei sämtlichen Sicherheitsüberlegungen, Lösungen und Massnahmen den Menschen in den Mittelpunkt zu stellen. Nur eine genau an die Bedürfnisse der Anwender angepasste Security wird mittel- und langfristig ihrer Aufgabe gerecht werden und die notwendige Resilienz schaffen.

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. Gepaart mit einer konsequenten Sicherheitskultur, Fehlertransparenz und gut ausgebildeten Mitarbeitenden schaffen sie 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.





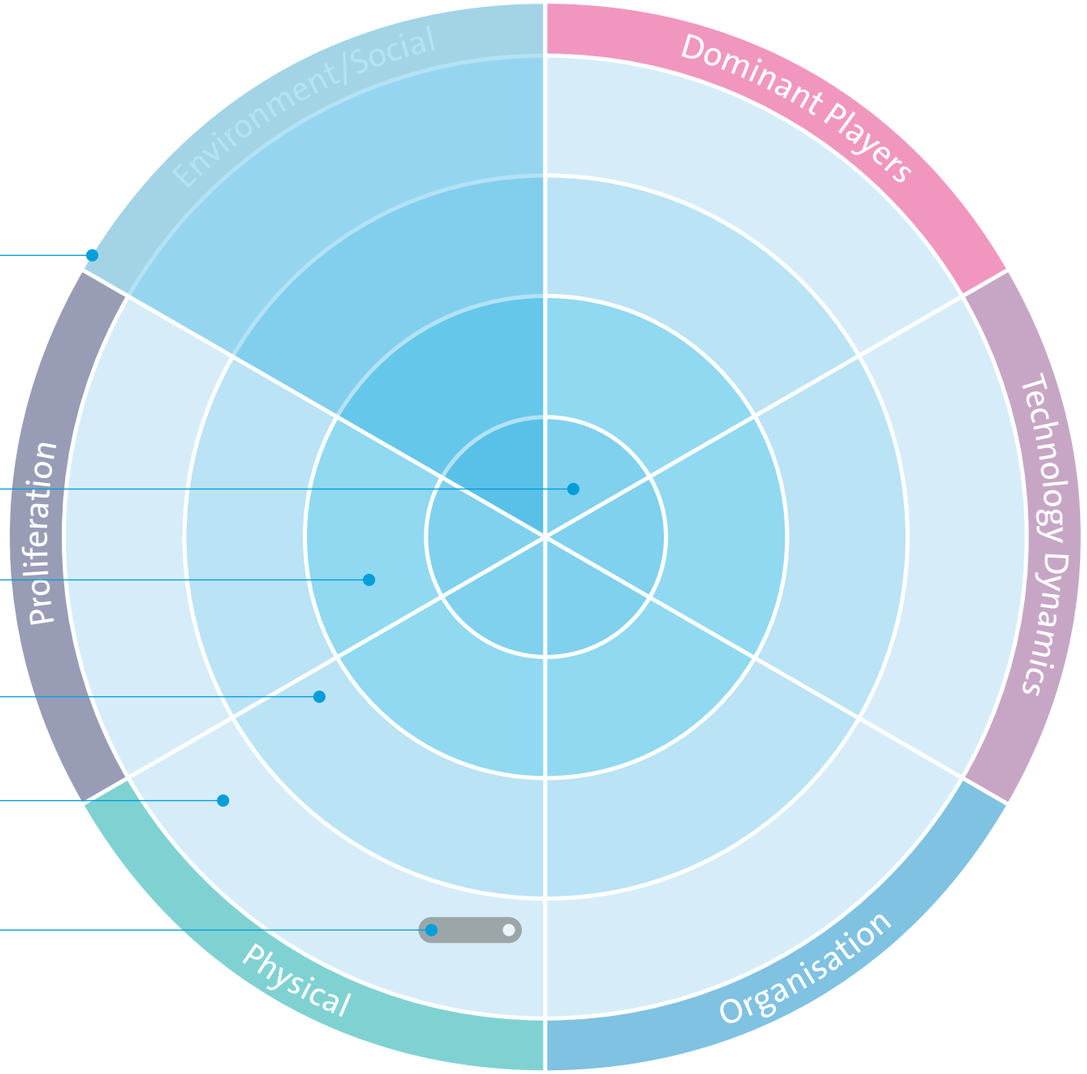
Methodik

Der Bedrohungsradar ist in sechs **Segmente** unterteilt, welche die unterschiedlichen Domänen der Bedrohungen voneinander abgrenzen. In jedem **Segment** können die dazugehörenden Bedrohungen einem von vier 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.

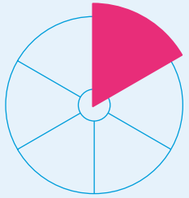
Die Kreise kennzeichnen wir als:

- **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.
- **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.
- **Beobachtung** für Bedrohungen, die erst in einigen Jahren eintreten werden. Es gibt noch keine konkreten Massnahmen für den Umgang mit diesen Bedrohungen.

Weiter weisen die einzelnen, durch benannte Punkte gekennzeichneten **Bedrohungen** einen **Trend** auf. Dieser kann in seiner Kritikalität zunehmend, rückläufig oder stabil sein. Die Länge des Trend-Strahls zeigt die erwartete Schnelligkeit auf, mit der sich die Kritikalität der Bedrohung ändern wird.

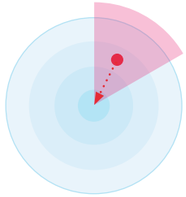


Details inkl. Trend und Vergleich zum Vorjahr



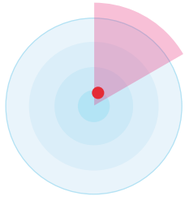
Dominant Players

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



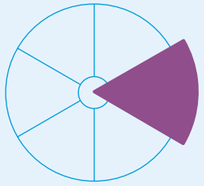
Concentration Data & Cloud Services
Die starke Zentralisierung von Daten in der Cloud führt zu Klumpenrisiken. Der Ausfall eines Service oder zentralen Dienstes kann weltweit Auswirkungen haben.

▲ **Zunehmend** (Hinweis: mehr dazu auf Seite 28)



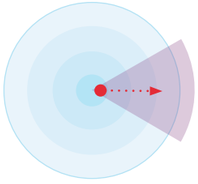
Infrastructure Integrity
In wesentliche Komponenten kritischer Infrastrukturen können fahrlässig oder bewusst Schwachstellen eingebaut worden sein, welche die Systemsicherheit gefährden.

► Unverändert



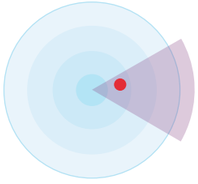
Technology Dynamics

Unter diesem Begriff sind Bedrohungen zu verstehen, die von der rasanten technologischen Innovation ausgehen und damit einerseits den Angreifern neue Möglichkeiten bieten, andererseits durch die eigene Entwicklung neue Bedrohungen schaffen.



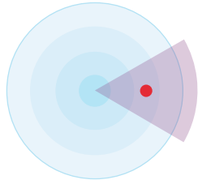
5G Security
5G ist eine noch junge Mobilfunktechnologie. Die Einführung wird neben vielen Chancen auch noch unbekannte Bedrohungen mit sich bringen.

▼ Abnehmend



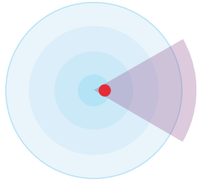
Automatisation & Scaling
Die stärkere Automatisierung technischer Betriebsprozesse wird bei erfolgreichen Angriffen oder Fehlkonfigurationen grössere Auswirkungen haben.

► Unverändert



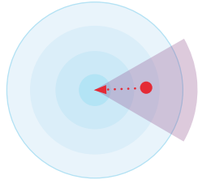
Quantum Computing
Quantencomputer können bestehende kryptografische Verfahren unbrauchbar machen, da sie diese in kürzester Zeit umgehen können.

▼ Abnehmend



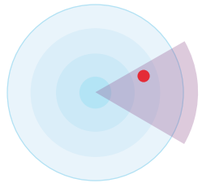
Ransomware
Kritische Daten werden grossflächig verschlüsselt und gegen Lösegeld (möglicherweise) wieder entschlüsselt.

▲ Zunehmend (Hinweis: mehr dazu auf Seite 32)



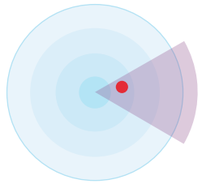
Increased Complexity
Die Komplexität von Systemen, insbesondere über Technologie- und Unternehmensgrenzen hinweg, nimmt laufend zu. Gerade im Hybrid-/Multi-Cloud-Umfeld mit vielen Cloud-Anbietern werden IT-Landschaften komplexer. Dadurch steigt die Risikoexposition und die Fehlersuche wird erschwert.

▲ Zunehmend



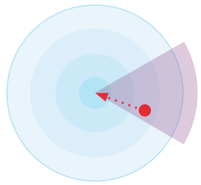
AI-Based Attacks
Angriffe mittels künstlicher Intelligenz (KI) sind gezielter und dadurch schwerer erkennbar. Durch KI können Angriffe effizienter auf klassische Angriffsvektoren wie z. B. Ransomware, Phishing, Spear-Phishing und vereinzelt auch auf neue Szenarien wie z. B. Deepfakes, Desinformation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

► Unverändert



Targeted Attacks (APTs)
Gezielte und komplexe Angriffe, um ein konkretes Ziel zu erreichen. Schlüsselpersonen werden identifiziert und gezielt direkt oder indirekt (lateral movement) 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.

► 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.

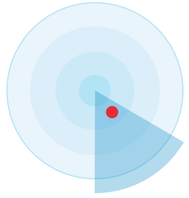
▲ **Zunehmend** (Hinweis: mehr dazu auf Seite 36)

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

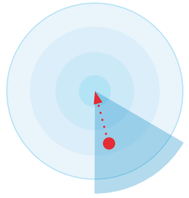


Decentralised Development & Operations
Klassische Entwicklungsabteilungen «sterben aus» und die Applikationsentwicklung rückt näher an die Business Units bei gleichzeitig kürzer werdenden Release-Zyklen heran. Dadurch wird die Kontrolle/Steuerung der Sicherheit erschwert.

► Unverändert

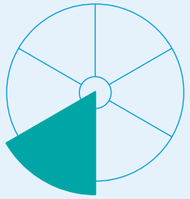
Insider Threat
Partner oder Mitarbeitende manipulieren, missbrauchen oder verkaufen Informationen fahrlässig oder vorsätzlich.

► Unverändert



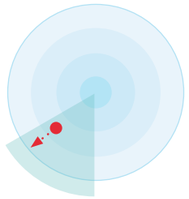
Infrastructure Misconfiguration
Ausnutzung von fehlkonfigurierten Infrastrukturkomponenten und/oder von Schwachstellen, die spät identifiziert und behoben werden.

▲ Zunehmend



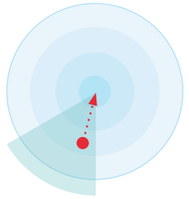
Physical

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.



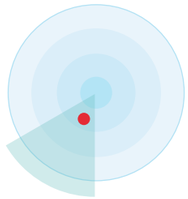
Device Theft
Der Diebstahl oder anderweitige Verlust von Endgeräten wie Smartphones, Laptops aber auch von relevanten IT-Komponenten kann zu Datenverlust führen oder die Verfügbarkeit der IT-Services beeinträchtigen.

▼ Abnehmend



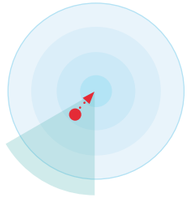
Energy Instability
Angriffe auf kritische Infrastrukturen wie Stromnetzbetreiber. Die Ausfallsicherheit ist essenziell und Business Continuity wird verstärkt auch in der Cyber-Resilienz-Debatte thematisiert. Strommangellage, Blackout (flächendeckender Stromausfall) oder gar Blueout (flächendeckender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

▲ Zunehmend



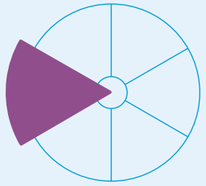
IoT-Devices
Schwach geschützte Geräte können kompromittiert und sabotiert werden. So können sie in der eigenen Funktion, z. B. der Verfügbarkeit oder Datenintegrität, eingeschränkt werden.

► Unverändert



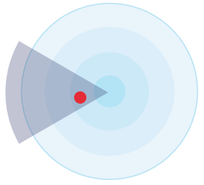
Betriebstechnologie OT
Betriebstechnologie (OT) ist die Verwendung von Hardware und Software zur Überwachung und Steuerung von physischen Prozessen, Geräten und Infrastrukturen. OT findet sich in einer Vielzahl von anlagenintensiven Sektoren und erfüllt verschiedenste Aufgaben, die von der Überwachung kritischer Infrastrukturen (CI) bis hin zur Steuerung von Robotern in einer Werkshalle reichen. Es existieren nach wie vor viele schlecht oder gar nicht geschützte Kontrollsysteme für Anlagen der kritischen Infrastruktur.

▲ Zunehmend



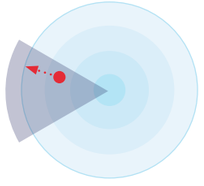
Proliferation

Bedrohungen, die von der immer einfacheren und günstigeren Verfügbarkeit von IT-Medien und -Know-how profitieren, fallen unter das Segment «Proliferation». Die weite Verbreitung führt zu mehr Angriffsflächen und erhöht die Verfügbarkeit von Angriffswerkzeugen.



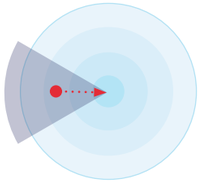
Digitalisation
Immer stärkere Vernetzung der realen und der virtuellen Welt im Privat- und im Geschäftsleben führt zu mehr Angriffswegen. Auch das neue «New Work» und das Verschieben der Arbeit in Homeoffice-Umgebungen erhöhen das Cyberrisiko und die Angreifbarkeit der IT-Infrastruktur über ungesicherte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

► Unverändert



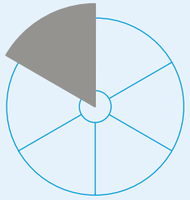
Subscriber Compromise
Schadsoftware verschafft sich Zugriff auf private Daten der Mobilnutzer oder wird für Angriffe auf die Telekommunikations- bzw. IT-Infrastruktur genutzt.

▼ Abnehmend



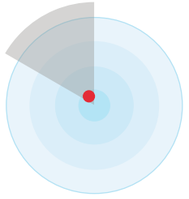
DDoS Attacks
Ein Denial-of-Service(DDoS)-Angriff ist ein böswilliger Versuch, den normalen Datenverkehr eines Zielservers, -dienstes oder -netzwerks zu stören, indem das Ziel oder die umgebende Infrastruktur mit einer Flut von Internetverkehr überschwemmt wird. DDoS-Angriffe erreichen ihre Effektivität,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

▲ Zunehmend



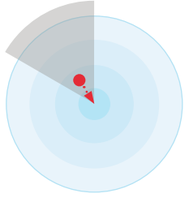
Environment/Social

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



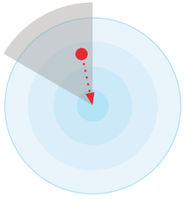
Security Job Market
Der Bedarf an Security-Professionals ist enorm gross und kann nur sehr schwer gedeckt werden. Dies führt zu einem abnehmenden Know-how im Kampf gegen immer komplexere und intelligentere Angriffe.

► Unverändert (Hinweis: mehr dazu auf Seite 24)



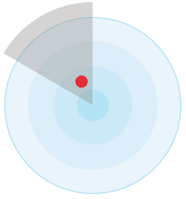
Digital Identity
Beglaubigte, persönliche digitale Identitäten können missbraucht oder gestohlen werden, um z. B. unter fremdem Namen Verträge abzuschliessen.

▲ Zunehmend



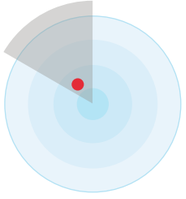
Desinformation & Destabilisation
Die absichtliche Verbreitung von unwahren Informationen kann zu einer wirtschaftlichen und gesellschaftlichen Destabilisierung führen und wird gerade in Krisenszenarien vermehrt auch über den Cyberraum gezielt eingesetzt.

▲ Zunehmend



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

► Unverändert



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

► Unverändert

Herausforderungen und Trends:
Fachkräftemangel im Security Job Market

Worum gehts?

Hybride, zunehmend dezentrale IT-Infrastrukturen, IoT-Umgebungen und Remote-Arbeit: Die Anforderungen an IT-Sicherheitssysteme wachsen, Bedrohungen nehmen zu, Fachkräfte aber sind rar. Unternehmen sollten mehrere Massnahmen bündeln, um Netzwerke und Daten zu schützen und Knowhow aufzubauen. Automatisierung sowie Aus- und Weiterbildung spielen zudem eine Rolle.

Die aktuellen Herausforderungen in der IT-Sicherheit werden durch einen Mangel an qualifizierten Fachkräften verschärft. Im Global Risk Report 2022 des WEF wird auch auf den weltweiten Mangel an Cybersecurity-Experten hingewiesen. Es wird geschätzt, dass rund drei Millionen Fachkräfte auf dem Arbeitsmarkt fehlen.

Wozu Personalknappheit in der Cybersicherheit führen kann, hat das International Information System Security Certification Consortium (ISC)² erfragt. 32 % der Befragten nennen fehlkonfigurierte Systeme als eine mögliche Folge. Nahezu ebenso viele fürchten, dass nicht genügend Zeit bleibt für ein angemessenes Risikomanagement oder dass etwas Wichtiges übersehen wird. 27 % berichten, dass es ihnen unmöglich sei, alle Bedrohungen des Netzwerks zu identifizieren. Ebenfalls 27 % halten eine aufgrund des Personalmangels überstürzte Installation und Konfiguration von Software für eine reale Gefahr.

Die Studie «ICT-Fachkräftesituation: Bedarfsprognose 2028» von ICT-Berufsbildung Schweiz prognostiziert, dass bis 2028 rund 118 000 zusätzliche ICT-Fachkräfte in der Schweiz benötigt werden. Will man diesen zusätzlichen Bedarf decken, müssten rund 36 000 Personen mehr ausgebildet werden, als es heute der Fall ist. Dies ist eine bildungspolitische und gesamtwirtschaftliche Herausforderung, die nach ausserordentlichen Massnahmen verlangt. Unternehmen aller Branchen sowie die öffentliche Verwaltung sind gefordert, neue Lehrstellen und Studienplätze in der Informatik und Mediamatik zu schaffen.

Angesichts solcher Zahlen ist es kein Wunder, dass es Unternehmen schwer fällt, geeignete Kandidaten zu finden und zu halten. Im Schnitt dauert es sechs Monate und erfordert etliche Ausschreibungen und Bewerbungsgespräche, um eine vakante Stelle in der IT zu besetzen. Zudem fällt es vor allem kleinen und mittleren Unternehmen nicht nur schwer, Spezialisten zu finden, sondern diese auch über längere Zeit genügend zu fordern und dadurch auch zu halten.

Wie wird sich die Herausforderung weiter entwickeln?

Die Einstellung von IT-Spezialisten ist eine Herausforderung, wenn nicht in genügendem Masse qualifizierte und geeignete Fachkräfte zur Verfügung stehen. Viele Unternehmen versuchen deshalb, das bereits eingestellte Personal zu halten. Damit allein wird das Problem aber nicht aus der Welt zu schaffen sein: Die Lösung für diese Herausforderungen wird darin bestehen, qualifizierte Mitarbeitende zu halten und die alltäglichen Aufgaben zu automatisieren.

Die Herausforderung, die richtigen Fachleute mit IT-Security-Skills für das eigene Unternehmen zu finden, wird weiter zunehmen, da mehr (auch kleinere) Firmen Experten benötigen. Durch den demografischen Wandel auf dem Arbeitsmarkt wird die Situation zusätzlich verschärft. Unternehmen haben immer weniger Zugriff auf neue und junge Fachkräfte. Der «War of Talents» wird sich intensivieren und die Sicherheitsbedürfnisse werden allgemein zunehmen. Krisenszenarien wie der Krieg in der Ukraine werden das Sicherheitsbewusstsein in den Unternehmen und Organisationen weiter steigern und stärken.

Der Fachkräftemangel im Bereich Cyber Security wird sich dabei in zweierlei Hinsicht bemerkbar machen: Zum einen fehlen die digitalen Experten bei der Entwicklung von IT-Security-Lösungen, während die Cybercrime-Attacken immer ausgefeilter und zielgerichteter werden. Zum anderen fehlen in den Unternehmen qualifizierte IT-Sicherheitsbeauftragte, die der steigenden Bedrohung durch Cyberkriminalität mit entsprechenden Massnahmen begegnen könnten.

Der IT-Fachkräftemangel trifft vor allem kleine und mittelständische Unternehmen (KMU), da qualifizierte Mitarbeitende grosse Konzerne mit attraktiveren Gehaltsmodellen und/oder Social Benefits den kleineren Betrieben häufig vorziehen.

Um den Personalmangel zu entschärfen, bieten immer mehr Universitäten spezielle Studiengänge für Cyber Security an. Ob sich die strukturellen Probleme dadurch schnell lösen lassen, bleibt allerdings fraglich. Bis das nötige Know-how aufgebaut ist, braucht es viel Zeit und neben der rein theoretischen Ausbildung auch eine gewisse Praxiserfahrung. Erfolgsversprechender könnte ein Ansatz sein, bei dem sich Unternehmen mit ihren Fachabteilungen und Spezialisten praxisnah in Forschung und Lehre engagieren. Zum anderen sollten Unternehmen auch auf interessierte Mitarbeitende setzen, indem sie sich verstärkt auf deren Fortbildung im Bereich Cyber Security konzentrieren. Zumindest mittel- und kurzfristig wird das aber wohl nicht ausreichen, um die klaffende Personal- und damit einhergehende Sicherheitslücke zu schliessen. In unterbesetzten Security-Abteilungen mangelt es nicht nur an Spezialwissen, meist arbeiten die Experten auch noch hart an der Belastungsgrenze, was natürlich keine gesunde Grundlage für die eigene Cyber Security ist.

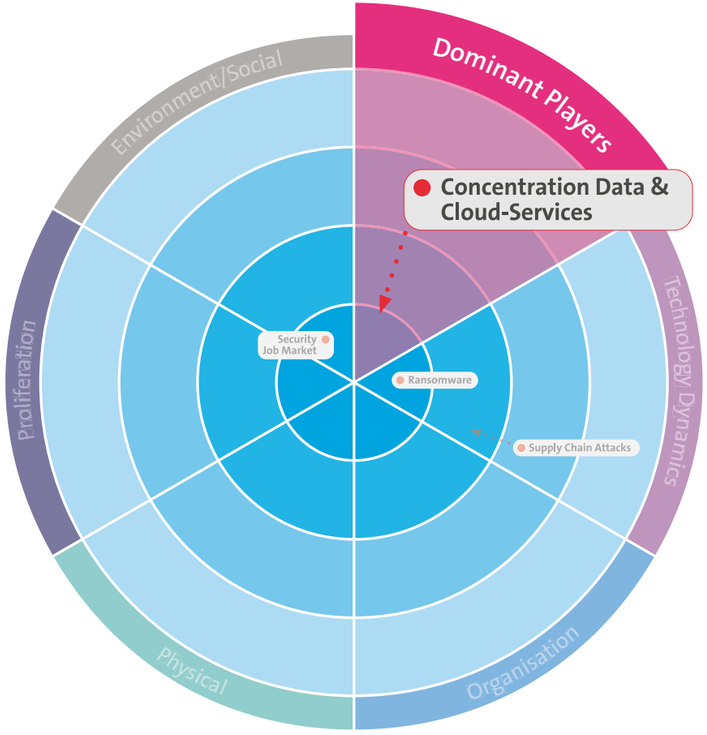
Wie kann man der Herausforderung wirkungsvoll begegnen?

- Attraktivität des Arbeitgebers hochhalten und Mitarbeitende ans Unternehmen binden
- Talente brauchen praxisnahe Förderung
- In die interne Fachausbildung investieren und attraktive Ausbildungsprogramme etablieren
- Entwicklungsmöglichkeiten im Unternehmen und eine hohe Arbeitsmarktfähigkeit bieten
- Im Recruiting Social Media stärker nutzen und an Fachevents Präsenz zeigen
- Employer Brand Marketing und das Netzwerk der Mitarbeitenden nutzen
- Juniorprogramme installieren bzw. Möglichkeiten für Juniors fördern (die zukünftigen Mitarbeitenden fit machen)
- Auch interne Bug Bounty Programme können Talente ausfindig machen
- Automatisierung von Standardprozessen und Software-Unterstützung auch bei komplexen Aufgaben
- Integration eines externen MSSP (Managed Security Service Provider)

«Es braucht nicht immer voll ausgebildete Experten. Wir machen gute Erfahrungen mit Profis aus benachbarten Expertise-Feldern (Entwickler, Netzwerkadmins u. ä.) und jungen Leuten nach der Ausbildung, die sich im Thema weiterbilden wollen.»

Dimosthenis Georgokitsos
Program Manager Cyber Security,
Recruiting & Education, Swisscom (Schweiz) AG

Herausforderungen und Trends:
Hybrid-/Multi-Cloud in Concentration Data & Cloud-Services



Worum gehts?

In einer Multi-Cloud-Lösung nutzt ein Unternehmen mehrere verschiedene Cloud-Services, oft von mehreren Anbietern. Die Multi-Cloud bietet Flexibilität und Wahlmöglichkeiten, führt aber auch zu Komplexität. Die «richtige» Cloud-Lösung ist für die meisten Unternehmen jedoch weder public noch private, sondern eine Kombination von beidem.

Multi-Cloud ist Teil der Reise in die Cloud. Nach einer erfolgreichen Migration und/oder dem Onboarding von Cloud-Diensten wird die Erkenntnis, dass eine weitere Cloud benötigt wird, zur Notwendigkeit. Dafür gibt es mehrere Gründe, z. B. Risiko; Lock-in; Dienste; Projekte; dezentralisierte DevOps-Teams, die verschiedene Cloud-Plattformen nutzen. Meistens handelt es sich um eine Multi-Azure-, GCP- oder AWS Cloud-Umgebung. Die zugrunde liegenden Dienste müssen mehrfach verwaltet werden, was zu Ineffizienz führt. Eine Dachlösung für mehrere Clouds kann einige Lösungen bieten, aber die Gesamtkomplexität wird zu einer neuen Herausforderung.

Eine Multi-Cloud-Strategie umfasst zwei oder mehr Cloud-Computing-Plattformen oder -Anbieter. Einige Fachleute würden nur dann von Multi-Cloud sprechen, wenn ein Unternehmen funktionsgleiche Dienste verschiedener Anbieter nutzt – im Gegensatz zu einer Strategie, bei der sich eine Organisation bei jedem Anbieter die Rosinen herauspickt.

Die meisten Studien/Experten weisen auf die folgenden Herausforderungen hin:

- Zentrales Identitäts- und Zugriffsmanagement über den gesamten Lebenszyklus
- Compliance
- Mangelnde Sichtbarkeit und Kontrolle (E2E)
- Datensicherheit
- Erhöhte Komplexität
- Wissens- und Kompetenzlücke
- Uneinheitliche Protokollierungs- und Überwachungsmöglichkeiten
- Sicherheit in der Lieferkette
- Verlagerung der Sicherheitsverantwortung

Wie wird sich die Herausforderung weiter entwickeln?

Zentralisiertes Identitäts- und Zugriffsmanagement (Identity and Access Lifecycle Management) wird noch wichtiger werden, da der Bedarf an Datensicherheit und Compliance weiter stetig steigen wird. Das Thema «End-To-End-Sichtbarkeit» muss für die Vorbereitung von Incident Detection & Response geklärt werden.

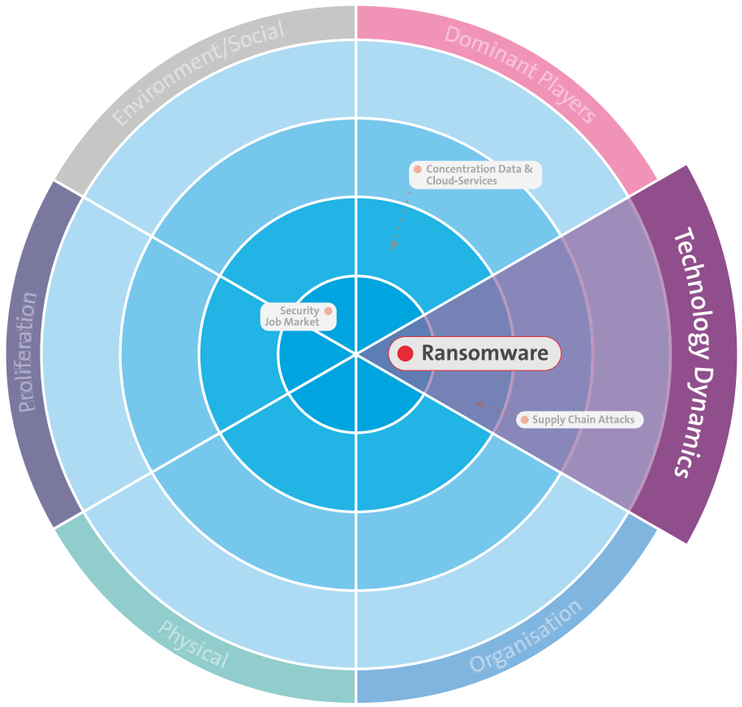
Wie kann man der Herausforderung wirkungsvoll begegnen?

- Frühzeitiges Denken in Richtung Multi-Cloud
- Eine Gesamtarchitektur, die den Wechsel von der Cloud zur Multi-Cloud ermöglicht
- Ein System zur Überprüfung der Sicherheitslage (Security Posture) und der Compliance über alle Clouds hinweg einsetzen
- Cloud-Infrastrukturen global überwachen und eine zentrale Übersicht über alle sicherheitsrelevanten Events erstellen

«Eine Multi-Cloud-Umgebung bietet unbestreitbare Vorteile. Die daraus resultierende Komplexität muss jedoch richtig gehandhabt werden, um die Risiken zu beherrschen, die mit der Zunahme der Angriffsfläche verbunden sind.»

Duilio Hochstrasser
Security Specialist, Swisscom (Schweiz) AG

Herausforderungen und Trends:
Ransomware



Worum gehts?

Ransomware ist eine Malware, die entwickelt wurde, um einem Benutzer oder einer Organisation den Zugriff auf die eigenen Dateien zu verunmöglichen. Indem sie diese Dateien mit Ransomware verschlüsseln und eine Lösegeldzahlung für den Entschlüsselungsschlüssel fordern, bringen Cyberangreifer Unternehmen in eine Position, in der die Zahlung des Lösegelds als der einfachste und billigste Weg erscheint, um wieder Zugriff auf ihre Dateien zu erhalten. Manchmal kommt noch Datendiebstahl dazu, um Ransomware-Opfer zusätzlich unter Druck zu setzen, damit sie Lösegeld zahlen.

Ransomware hat sich schnell zur bekanntesten und sichtbarsten Art von Malware entwickelt und verursacht weltweit jährliche Kosten von über 1 Milliarde US-Dollar (Gartner). Da Ransomware zu einer lukrativen Geschäftsoption für Cyberkriminelle geworden ist und die Angriffsmethoden immer weiter an Raffinesse zunehmen, werden die durch die Angriffe verursachten Kosten weiter steigen. Während bis vor Kurzem vor allem Grosskonzerne vor Angriffen mit Ransomware zitterten, trifft es in den letzten Jahren auch immer mehr den Mittelstand.

Dabei sind es nicht nur die direkten Kosten – wenn ein Unternehmen auch tatsächlich das Lösegeld zahlt –, die bei einem Angriff auf ein kleines Unternehmen durchschnittlich um die 710 000 CHF betragen, sondern auch die indirekten Kosten für Geschäftsausfälle während der Stunden/Tage, in/an denen die Systeme gesperrt sind. Dazu kommen die Kosten für die Reparatur oder Wiederherstellung der Systeme plus der Imageschaden. Ein schlechter Ruf kann Unternehmen innert kürzester Zeit in eine existenzielle Notlage bringen. Der Wiederaufbau der Reputation kostet sehr viel Energie, Zeit und Geld.

Wie wird sich die Herausforderung weiter entwickeln?

Der Trend ist ungebrochen. Solange ungepatchte Systeme oder RAS-/VPN-Zugänge ohne Multi-Faktor-Authentifizierung (MFA) im Internet erreichbar sind und Mitarbeitende Malware wie Quakbot installieren, ist das Risiko einer Ransomware-Attacke gegeben. Aufgrund von einfach durchführbaren und oft erfolgreich verlaufenden Phishing-/Malspam-Manövern ist eine Weiterentwicklung erfolgreicher Ransomware-Angriffe seitens Cyberkrimineller gar nicht nötig. Eventuell werden Angriffe künftig vermehrt automatisiert oder weiter «As-a-Service» organisiert. Deepfake-Technologien und der Einsatz von Künstlicher Intelligenz (KI) werden diese Angriffe noch schwerer identifizierbar machen. Zudem zeichnet sich ab, dass immer mehr Angreifer die Daten nicht nur verschlüsseln, sondern auch mit einer Veröffentlichung derer drohen («Double Extortion»).

In der EU müssen Unternehmen ab Mitte 2023 Ransomware-Attacken melden. Deshalb muss davon ausgegangen werden, dass sich die Anzahl der öffentlich bekannt werdenden Angriffe massiv erhöhen und dadurch in der Bevölkerung das Gefühl aufkommen wird, dass die Anzahl der Angriffe zugenommen hat. Ob dies Einfluss auf die effektive Anzahl der Angriffe nehmen wird, kann daraus nicht abgeleitet werden. Klar ist: Ransomware ist keine «höhere Gewalt» und man muss zukünftig sicher damit rechnen, dass auch Cloud-Services von Cyberkriminellen in «Gefangenschaft» genommen werden.

Wir und vergleichbare Industrien arbeiten mit Hochdruck an der Verbesserung ihres Umgangs mit Ransomware.

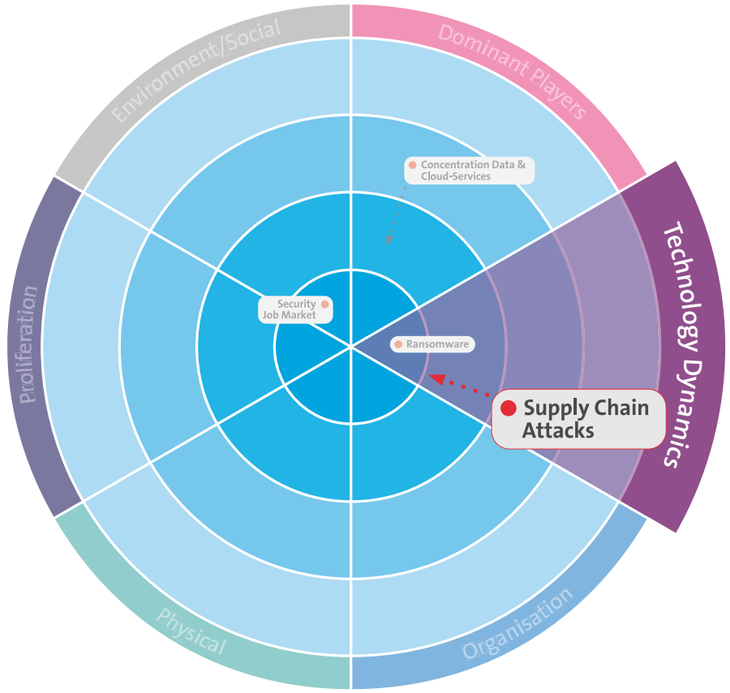
Wie kann man der Herausforderung wirkungsvoll begegnen?

- Sicherstellen, dass die Verwaltung von IT-Systemen und Softwareanwendungen in der gesamten Organisation ordnungsgemäss gehandhabt wird
- Alle Internet-facing Services zeitnah patchen (insbesondere, wenn die Schwachstellen schon ausgenutzt werden)
- Regelmässig (offline) Backups von Systemen & Daten erstellen (und das Recovery dieser Back-ups testen)
- Entwicklung eines Krisenkommunikationsplans, der Drittanbieter, Lieferanten, Partner, Mitarbeitende und andere wichtige Interessengruppen berücksichtigt
- Bewertung der Fähigkeit des Unternehmens (und der IT-Abteilung), auf einen Angriff reagieren und mögliche Systemausfälle mithilfe von Response-Plänen bewältigen zu können
- Sicherstellen, dass die Mitarbeitenden angemessen über Cybersicherheit und die Gefahr eines Ransomware-Angriffs aufgeklärt werden
- RAS-/VPN-Services mit Multi-Faktor-Authentifizierung (MFA)/Conditional Access schützen
- In ein flächendeckend ausgerolltes EDR und Monitoring (z. B. der Active-Directory-Infrastruktur) investieren. So hat man eventuell noch die Chance, den Angriff rechtzeitig zu erkennen und zu stoppen
- Angriffsfläche verringern

«Ransomware-Angreifer verhalten sich opportunistisch. Sie greifen dort an, wo sich eine Gelegenheit bietet, also ein Zugang vorhanden ist.»

Thomas Röthlisberger
Senior Security Analyst & Tech Lead Red Team im Swisscom CSIRT

Herausforderungen und Trends:
Supplier Ecosystem and Dependencies / Supply Chain Security



Worum gehts?

Alle Organisationen müssen ein gewisses Mass an Vertrauen in andere Unternehmen haben, wenn sie die Software der jeweiligen Unternehmen in ihren Netzwerken installieren und mit ihnen zusammenarbeiten. Ein Supply-Chain-Angriff nutzt genau diese Vertrauensbeziehungen – aber auch den Verlust der Kontrolle aufgrund von Abhängigkeiten zwischen verschiedenen Organisationen – aus.

Der Angriff zielt dabei auf das schwächste Glied in einer Vertrauenskette ab. Wenn eine Organisation über eine starke Cybersicherheit verfügt, aber mit einem unsicheren Anbieter zusammenarbeitet, werden die Angreifer diesen Anbieter ins Visier nehmen. Mit einem Standbein im Netzwerk des Anbieters können die Angreifer dann über diese vertrauensvolle Beziehung zum sichereren Netzwerk wechseln. Störungen bei Lieferanten gefährden die eigene Leistungserbringung z. B durch fehlende Vorleistungen (SLA-Bruch auf unserer Seite) oder durch direkte Gefährdung von uns (z. B. durch Kompromittierung von Fremdgeräten in unseren Netzwerken oder Software).

Denn eine gängige Art von Angriffszielen in der Lieferkette sind Managed Service Provider (MSPs). MSPs haben umfassenden Zugriff auf die Netzwerke ihrer Kunden, was für Angreifer von unschätzbarem Wert ist. Nach der Ausnutzung des MSP können Angreifer ihre Aktivitäten leicht auf Kundennetzwerke ausweiten. Durch die Ausnutzung von Schwachstellen in der Lieferkette haben diese Angreifer einen grösseren Einfluss und können Zugang zu Netzwerken erhalten, die sonst viel schwieriger anzugreifen wären. Auf diese Weise gelang es den Kaseya-Angreifern, dermassen viele Organisationen mit Ransomware zu infizieren.

Andere Supply-Chain-Angriffe erfolgen mit einer Software, die Malware an die Kunden eines Unternehmens liefert. Beispielsweise verschafften sich die Angreifer von Solarwinds Zugriff auf die Build-Server des Unternehmens und fügten eine Hintertür in Updates des Netzwerküberwachungsprodukts Solarwinds Orion ein. Nachdem dieser Update-Code an Kunden weitergegeben wurde, verschafften sich die Angreifer so auch Zugriff auf deren Netzwerke. Log4J hat zudem gezeigt, dass viele Unternehmen ein ungenügendes Verständnis der Verwendung von Libraries und Frameworks in Lösungen haben. Dies geht über die direkten Lieferanten hinaus und schliesst Sub- oder Subsub-Lieferanten ein.

Wie wird sich die Herausforderung weiter entwickeln?

Wir rechnen mit einer Zunahme dieser Herausforderung infolge stärkerer Vernetzung mit Lieferanten (Remotesupport; Softwarebibliotheken; SaaS) und gezielten Angriffen zur Störung von Lieferketten. Zudem nutzen Angreifer heute viel rascher entdeckte Lücken aus.

Wie kann man der Herausforderung wirkungsvoll begegnen?

- Konzentration auf die wichtigsten/kritischsten Lieferanten
- Integration von DevSecOps-Techniken in den Entwicklungslebenszyklus
- Datenminimierung im Austausch mit Partnern
- Inventarisierung der Lieferantenbeziehungen und Beurteilung ihrer Auswirkungen
- Kontinuierliche Beobachtung wichtiger Lieferanten und Erstellung von Continuity-Plänen
- Aufbau von Alternativen und Ausweichlösungen für wichtige Lieferanten

«Mit nachweislichen «Software Bills of Materials» (SBOM) lässt sich die Zusammensetzung von Lieferobjekten bis auf Funktionsstufen prüfen und verifizieren – auch über mehrere Stufen. Das Gleiche ist auf Hardwarestufe für Custom- aber auch für Standard-Hardware durchgehend durchzuführen. Teilweise ist es in gewissen Technologien heute schon verfügbar.»

Oliver Jäschke
Security Governance Manager, Swisscom (Schweiz) AG

Fazit

Dachten wir, durch einen allmählichen Rückgang der besonderen pandemischen Lage kehrt ein wenig Ruhe ein, zeigt sich durch den Krieg in der Ukraine erneut die Vulnerabilität unserer Welt. Vieles wirkt heute noch zerbrechlicher und unbeherrschbarer.

Dazu kommt der immer stärker bemerkbare Ressourcenmangel in vielen IT- und Security-Abteilungen. Die Welt sieht sich mit «Wicked Problems» konfrontiert, also mit Problemen, die aufgrund unvollständiger, widersprüchlicher und sich ändernder Anforderungen schwer erkennbar, nicht immer vorhersehbar, planbar und mitigierbar und dadurch in der Regel nur schwer oder unmöglich zu lösen sind.

Das klingt alles vertrackt und kommt mit einer leicht deprimierenden Note daher – aber davon brauchen wir uns nicht entmutigen zu lassen. Die Digitalisierung in Unternehmen und Organisationen schreitet mutig voran. Die Verlagerung von IT-Komponenten und IT-Services in die Cloud steht bei fast allen Organisationen und Unternehmen auf der IT-Agenda für 2022 – oder stand es schon in den letzten Jahren. Themen wie Metaverse, Web 3.0, NFTs und Blockchain prägen die aktuelle Entwicklung im Cyberraum und geben Anlass zur Hoffnung. Hier gilt es dranzubleiben, abzuwägen und ein aktives Risikomanagement zu betreiben.

Wir müssen in der zunehmend volatileren, unsichereren, komplexeren und mehrdeutigeren Welt einen grösseren Fokus auf unser eigenes Risikomanagement legen. Was gilt als schützenswert? Wer oder was bedroht unsere Werte und Assets in der Organisation? Welche Rolle spielen kritische Services und Komponenten von Dritten – Zulieferern, SaaS-Anbietern, Cloud-Diensten usw.?

Wir müssen die Mitarbeitenden zu Verbündeten machen, von den Führungskräften die so hoch beschworene Vorbildfunktion einfordern, die Einhaltung von Vorgaben und Regeln konsequent überwachen und Allianzen über Abteilungsgrenzen hinweg schaffen. Um den sich im ständigen Wandel befindlichen Risiken und Gefahren auch die entsprechende «Defense» entgegensetzen zu können, muss die Security agiler sein.

«Der Mensch spielt im Sicherheitsdispositiv die zentrale Rolle.»

Notizen

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	© Mai 2022 by Swisscom (Schweiz) AG, Group Security, Alte Tiefenaustrasse 6, 3048 Worblaufen, swisscom.ch
Druck	OK DIGITALDRUCK AG, Zürich
Auflage	200 Exemplare

Sorgenfrei in der vernetzten Welt

Wir stellen die Bedürfnisse unserer Mitarbeitenden, Kunden und Partner ins Zentrum aller Sicherheitsüberlegungen. Auf Basis modernster IT und Netze entwickeln wir sichere Lösungen, Produkte und Dienstleistungen.

Du suchst bei Swisscom einen Job im Security-Bereich?
Dann schau hier
und bewirb dich:

swisscom.com/securityjobs

#talkingaboutsecurity

swisscom.ch/security