swisscom

Cyber Security Threat Radar
2022/2023

Security by Design leben

Inhalt

«Sicherheit von Anfang an konsequent mitdenken und die Mitarbeitenden in den Fokus stellen, das verstehen wir unter Security by Design und Human Centered Security. Nur damit wird es uns gelingen, unsere Unternehmen sicherheitsseitig auf Kurs zu halten.»

Cyber Security Threat Radar

Cyberrisiken – gekommen, um zu bleiben?

Die Gefahr, die von Cyberrisiken ausgeht, bewegt sich weiterhin auf sehr hohem Niveau. Damit die Cyberresilienz im eigenen Unternehmen verbessert werden kann, ist es zwingend nötig, die Cyber- und IT-Sicherheit ganzheitlich zu betrachten. Krisen aussitzen oder darauf zu hoffen, dass sich die Bedrohungslage bald wieder normalisiert, ist nicht zu empfehlen. Vielmehr ist es ratsam, sich umfassend auf mögliche Krisenszenarien vorzubereiten, damit im Ernstfall möglichst adäquat und schadensminimierend damit umgegangen werden kann. Die Multi- und Cyberrisiken, mit denen wir uns aktuell konfrontiert sehen, sind gekommen, um zu bleiben. Ihr Impact ist in vielen Ländern rund um den Globus spür- und sichtbar. Die Gefahr besteht, dass sie durch Kollateralschäden noch unberechenbarer werden.

Mittlerweile sollte allen klar sein, dass das Thema Cybersicherheit nicht nur in der Verantwortung der IT-Abteilungen liegt, sondern sämtliche Bereiche eines Unternehmens betrifft. Ein fundiertes Business Continuity Management gehört zu einem Risikodispositiv genauso dazu wie eine stabile Service-IT. Neben den technischen Vorkehrungen spielen aber auch gut geschulte und aufmerksame Mitarbeitende eine zentrale Rolle. Nur in der Kombination ist eine maximale Resilienz zu erreichen.

Der vorliegende Cyber Security Threat Radar soll dabei helfen, die zentralen Cyberrisiken im eigenen Unternehmen zu identifizieren und angemessen zu bekämpfen. Er dient als Leitfaden, um ein einheitliches Problembewusstsein für Cybersicherheit zu schaffen und ein umfassendes Sicherheitskonzept etablieren zu können.

Diese organisationsübergreifende Orientierungshilfe schafft die Grundlage für eine erfolgreiche Cybersicherheit – und damit die Basis für den Erfolg eines jeden Unternehmens in der digitalen Welt.

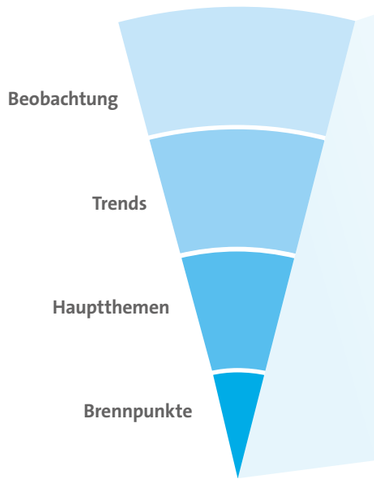
Marco Wyrsch
Head of Group Security
Swisscom (Schweiz) AG

«Der Krieg in Europa verändert gerade unsere Welt», sagte Philippe Vuilleumier, mein Vorgänger als Head of Group Security bei Swisscom, einleitend zum letztjährigen Cyber Security Threat Radar. Seine Aussage hat auch ein Jahr später an ihrer Gültigkeit nichts verloren, der Krieg hält die Welt immer noch in Atem. Die Auswirkungen sind in vielerlei Hinsicht spürbar: drohende Strommangellage, Gasknappheit, Verlagerung von Kriegsaktivitäten in den Cyberraum, Sabotageakte auf kritische Infrastrukturen, jede Menge Fake News und eine intensive Medienberichterstattung über alle Kanäle hinweg. Die derzeitige Situation macht deutlich, dass logische und physische Sicherheit in Zeiten von Multikrisen Hand in Hand gehen. Umso wichtiger ist ein geschärftes Risikobewusstsein. Das Zusammenspiel von Menschen, Prozessen und Technologien bildet das Fundament, um damit eine unternehmerische Resilienz und Stabilität in unsicheren Zeiten zu schaffen.

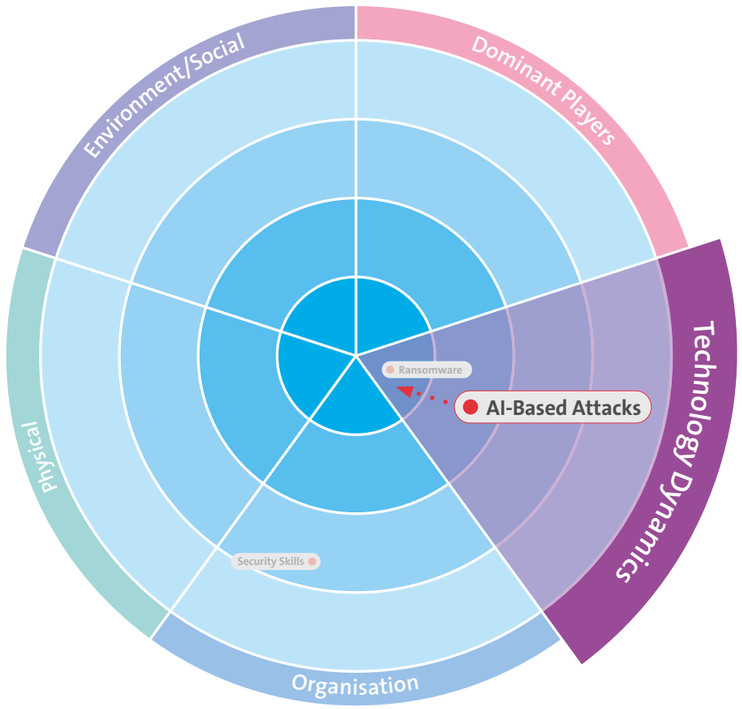
Lagebild – Bedrohungsradar

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 wir die Grundlage für eine organisationale Resilienz.

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



Herausforderungen und Tendenzen:
AI-Based Attacks – die dunkle Seite des technologischen Fortschritts



Worum gehts?

AI-Based Attacks (AI für artificial intelligence) sind Cyberangriffe, bei denen Künstliche-Intelligenz-Technologien eingesetzt werden, um Angriffe effektiver und effizienter zu gestalten oder um bestehende Abwehrmassnahmen zu umgehen.

Von KI-basierten Angriffen ist schon seit Längerem die Rede. In den letzten Monaten hat sich allerdings bei den verfügbaren Tools ein regelrechter Evolutionssprung gezeigt. Tools, wie die im November 2022 veröffentlichte Large Natural Language Model KI ChatGPT, zeigen eindrucksvoll, wie sich z.B. Phishing-Angriffe qualitativ signifikant verbessern oder zum Aufspüren von Schwachstellen in Programmcodes einsetzen lassen. Aktuell ist das Thema AI medial sehr präsent und deren Missbrauch für die Erstellung von Malware/Schadcodes und Phishing-Kampagnen wird künftig sicherlich zunehmen. Die Entwicklung wird von uns beobachtet und analysiert, ist aber aktuell noch kein «Hot Spot»-Thema.

Wie wird sich die Herausforderung weiterentwickeln?

Als eine der ersten Entwicklungen erwarten wir eine zunehmende Verschmelzung von zielgerichteten Angriffen mit KI-generierten Phishing-E-Mails. Eine Sprachmodell-KI kann auf Basis eines bestehenden E-Mail-Verlaufs eine überzeugende Story-Line für die Weiterführung der Konversation erstellen und geschickt mit einem Phishing- oder Social-Engineering-Angriff verbinden. Durch entsprechende Automatisierung lassen sich so gezielte Phishing-Kampagnen mit völlig individualisierten, kontextabhängigen E-Mails verfassen.

Eine weitere Entwicklungsrichtung für den schädlichen Einsatz von Sprachmodell-KIs ist deren Fähigkeit, Programmcodes auf Schwachstellen hin zu analysieren und Malware zur Ausnutzung der gefundenen Schwachstellen, inklusive geeigneter Angriffsvektoren, zu programmieren. Das notwendige Know-how von Angreifern zur Durchführung komplexer Angriffe sinkt so weiter.

Dazu kommt, dass durch die rasante Evolution von bild- und videogenerierenden KIs weiterhin Deep-Fake-Angriffe und -Desinformationskampagnen möglich werden, die mit herkömmlichen Mitteln kaum mehr zu identifizieren sind.

Wie kann man der Herausforderung wirkungsvoll begegnen?

Genauso wie KI-Technologien von Angreifern eingesetzt werden können, wird KI aber auch den Verteidigern bessere Möglichkeiten zur Erkennung und Abwehr von Cyberangriffen an die Hand geben, um z.B. KI-generierte Texte oder KI-generiertes Bild- und Videomaterial zu erkennen. Konzepte wie Zero Trust zum granular gesteuerten und authentifizierten Zugriff auf Daten und Ressourcen helfen, die Angriffsfläche von Unternehmen zu verringern.

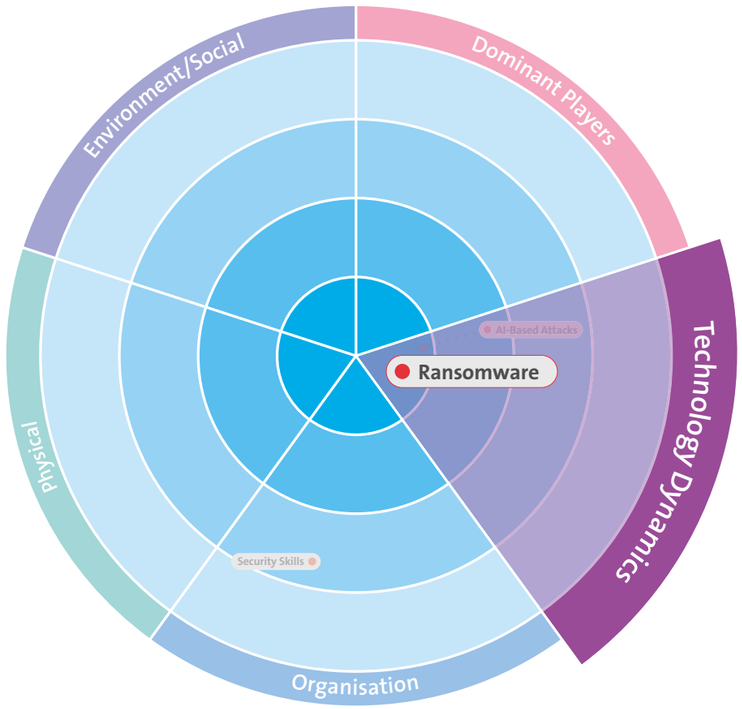
Aber auch etablierte Security Best Practices, wie die Multi-Faktor-Authentifizierung, DevSecOps, Vulnerability & Patch Management und Security Awareness bei Mitarbeitenden, helfen bei der Verhinderung von Cyberangriffen – nicht nur von KI-basierten Angriffen, sondern generell.

«Während sich KI-Technologien rasant weiterentwickeln, müssen wir uns bewusst sein, dass sie nicht per se gut oder böse sind. Es handelt sich dabei vielmehr um ein Werkzeug, das für beide Zwecke genutzt werden kann. Die Herausforderung besteht darin, die Verteidigung weiter so zu stärken, damit auch KI-basierte Angriffe erfolgreich abgewehrt werden können – zukünftig zunehmend auch mit der Hilfe von ‹guter› KI.»

Florian Leibenzeder
Leiter Swisscom Security Operation Center

Herausforderungen und Tendenzen:

Ransomware – Erpressung durch Datendiebstahl statt «nur» Verschlüsselung



Worum gehts?

Ransomware ist eine Art von Malware (Schadsoftware), die darauf abzielt, die Daten des Opfers nach der Infektion eines Computers, Servers oder Netzwerks zu verschlüsseln und somit für das Opfer unbrauchbar zu machen. Nur gegen die Zahlung eines Lösegelds («Ransom») erhält das Opfer den für die Entschlüsselung und damit für die Wiederherstellung der Daten benötigten Schlüssel. Auch im letzten Jahr wurde diese Angriffsform als akute Herausforderung erkannt und im Cyber Security Threat Radar gesondert adressiert.

Seitdem haben aber viele Unternehmen und Organisationen technisch aufgerüstet und sich weiterentwickelt, daher werden aufgrund von Ransomware-Attacken immer weniger Lösegelder bezahlt. Die Angreifer werden entweder schon beim Versuch der Verschlüsselung erfolgreich abgeblockt oder die Daten können auf andere Art und Weise wiederhergestellt werden. So gelingt es beispielsweise Angreifern oftmals nicht mehr, Backups unbrauchbar zu machen. Daher setzen sie vermehrt auf die Exfiltration von Daten und die anschliessende Drohung, diese zu veröffentlichen. Anders als bei verschlüsselten Daten, die man aus dem Backup wiederherstellen kann, ist es bei den exfiltrierten Daten nahezu unmöglich, eine Veröffentlichung, ohne die Zahlung von Lösegeld, zu verhindern.

Angreifer sind finanziell motiviert. Ransomware-Attacken und der damit verbundene Datendiebstahl sind für sie die einfachste und direkteste Methode, um aus einer kompromittierten Unternehmensinfrastruktur finanziellen Gewinn zu schlagen. Die geforderte Summe richtet sich üblicherweise nach der Grösse des Unternehmens und beträgt etwa drei Prozent des Umsatzes. Dabei gilt es jedoch, zu beachten, dass die bezahlte Lösegeldsumme oft nur einen Bruchteil der durch den Angriff verursachten Kosten darstellt.

Auch wenn es keine offiziellen Statistiken über die Höhe der tatsächlich getätigten Zahlungen gibt, gehen Schätzungen von einem durchschnittlichen Ertrag von 950 000 Schweizer Franken pro erfolgreichen Angriff aus.

Global wird der durch Ransomware-Attacken verursachte wirtschaftliche Schaden bis zum Jahr 2031 voraussichtlich 240 Milliarden Schweizer Franken übersteigen.

Die Aussicht auf das grosse Geld bei solchen Attacken führt zu einer zunehmenden Professionalisierung der Angreifer. In diesem Zusammenhang spricht man sogar von sogenannten Ransomware-Unicorns. Aus diversen Quellen, beispielsweise den Conti-Leaks, ist bekannt, dass viele Angreifer mittlerweile über ähnlich grosse finanzielle Mittel wie gut finanzierte IT-Startups verfügen.

So beschäftigen sie teilweise mehrere fest angestellte Entwickler und Hacker und bieten ihren Opfern mehrstufigen «Kundensupport» an. Sie nutzen agile Entwicklungsmethoden und entwickeln ihr Businessmodell und ihre Infrastruktur stetig weiter. Sie unterhalten auch eigene Bug-Bounty-Programme, mit deren Hilfe die Cyberkriminellen auf Sicherheitslücken in ihrer IT-Infrastruktur aufmerksam gemacht werden möchten.

Einige Hackergruppen legen zudem grossen Wert auf ihre Bekanntheit. So hat die Hackergruppe Lockbit in einer Guerilla-Marketing-Aktion dazu aufgerufen, sich gegen die Bezahlung von 1000 US-Dollar das Lockbit-Logo tätowieren zu lassen. Nach diesem Aufruf wurden im Internet viele Fotos gepostet, die Leute mit einem frisch gestochenen Lockbit-Tattoo zeigten.

Wie wird sich die Herausforderung weiterentwickeln?

Ransomware ist und bleibt ein Hot Topic. Wir erwarten eine deutliche Zunahme an Multiple Extortion, also der Verknüpfung mehrerer Angriffsformen wie Ransomware, Datendiebstahl und Denial-of-Service, da sich diese Form der Ransomware-Angriffe bei den Cyberkriminellen bereits etabliert hat. Auch Managed-Service-Provider gelangen mehr und mehr in den Fokus der Angreifer. Bei ihnen ist die Bereitschaft zur Lösegeldzahlung erfahrungsgemäss gross, zudem können auch ihre Kunden direkt attackiert werden, um noch mehr Profit aus dem Angriff herauszuschlagen.

Die grösste künftige Herausforderung stellt die zunehmende Spezialisierung der Angreifer und die damit einhergehende Komplexität ihrer Angriffe dar. Schon jetzt geht die grösste Bedrohung von sogenannten Ransomware-as-a-Service-Angeboten aus. Dabei dringen die Ransomware-Gruppen nicht mehr selbst in Unternehmen ein, sondern vermieten ihre Verschlüsselungs-Schadsoftware sowie ihre Server- und Supportinfrastruktur an andere Angreifer. Das erhaltene Lösegeld wird dann «brüderlich» zwischen den Angreifern und der Ransomware-Gruppe aufgeteilt. Es gibt «Initial Access Brokers», die sich darauf spezialisieren, in Unternehmen einzudringen und danach die gewonnenen Zugriffsmöglichkeiten zu verkaufen.

Der initiale Zugriff kann entweder über die Ebene Mensch oder die Ebene Infrastruktur beschafft werden: Auf Infrastrukturebene werden öffentlich erreichbare Server über bereits bekannte Vulnerabilities oder über «Zero-Day-Exploits» attackiert. Zero-Day-Exploits werden dabei häufig auch nicht mehr selbst entwickelt, sondern von anderen Parteien eingekauft.

Die Ebene Mensch wird von einigen Angreifern mit gezielten (Spear-)Phishing-Kampagnen auf die Endnutzer eines Unternehmens attackiert. Andere Ransomware-Gruppen kontaktieren die Mitarbeiter ihrer Opfer direkt und versuchen, diese durch die Zahlung hoher Geldsummen zu bestechen. Sogar Angriffe auf die private Infrastruktur von Mitarbeitern werden immer häufiger beobachtet, zuletzt bei den Angriffen auf Last Pass, bei denen zunächst das Heimnetzwerk eines Systemadministrators gehackt worden war, um dort die Zugangsdaten für das VPN des Unternehmens zu stehlen.

Wie kann man der Herausforderung wirkungsvoll begegnen?

Die wichtigste Schutzmassnahme ist, sich an etablierten Best Practices zu orientieren. Dazu gehören unter anderem:

- Patch & Vulnerability Management
- Einsatz moderner Air-Grapped-Backup-Lösungen und regelmässig erstellte (Offline-)Backups sowie regelmässiges Testen der Wiederherstellung
- Security Awareness innerhalb eines Unternehmens aufbauen
- Konsequent Multi-Faktor-Authentifizierung (MFA) einsetzen und gegen MFA-Fatigue absichern
- Flächendeckende Überwachung der IT-Sicherheit mittels Endpoint Detection and Response (EDR)
- Spezialisierte Sicherheitsteams wie Security Operation Centers (SOC) und Cyber Security Incident Response Teams (CSIRT)
- Netzwerksegmentierung und Sicherheitszonenkonzept
- Definieren von Incident Response und Krisenkommunikationsprozessen sowie regelmässige Trainings von möglichen Krisenszenarien

«Wenn sich Angreifer zunehmend spezialisieren, kann es sehr hilfreich sein, auch bei der eigenen Verteidigung auf spezialisierte Unternehmen und den Einsatz externer Expertenteams zu setzen.»

Tim Trinkl
Senior Security Analyst & Incident Responder B2B

Herausforderungen und Tendenzen:
Security Skills – dem Fachkräftemangel und einem Wissensverlust vorbeugen

Worum gehts?

Unabhängig von ihrer Grösse sehen sich zahlreiche Unternehmen oft mit derselben Herausforderung konfrontiert: Ihre Sicherheitsteams sind unterbesetzt und/oder schlichtweg überlastet. Die steigende Anzahl an Sicherheitsvorfällen, die Herausforderung, diese zu priorisieren, und der Mangel an Fachkräften kann Unternehmen überfordern und damit zu einem erhöhten Risiko führen. Um mit den Cyberkriminellen Schritt halten zu können, brauchen Unternehmen nicht unbedingt mehr Budget, sondern Mitarbeitende, die über eine einschlägige IT-Sicherheitsexpertise verfügen. Und hier sind gleich zwei im Cyber Security Threat Radar thematisierte Angriffsvektoren verortet: Security Skills und Infrastructure Misconfiguration. Durch fehlende Skills sowie fehlendes Personal steigen die Cyberrisiken durch die Ausnutzung von fehlkonfigurierten Infrastrukturkomponenten exponentiell.

Schweizer Universitäten, Fachhochschulen und anderswertige Ausbildungsinstitute haben in den letzten Jahren ihre Studienangebote massiv ausgebaut, sind aber noch nicht in der Lage, dem derzeit hohen Bedarf an Cyber-Security-Fachkräften gerecht zu werden.

In einem stetigen Kampf um Talente kann man sich als Unternehmen verausgaben und versuchen, den leergefischten Arbeitsmarkt zu bearbeiten. Eine andere Variante ist es, den Blick nach innen zu richten und in die Weiter- und Ausbildung der eigenen Mitarbeitenden zu investieren. Angesichts der steigenden Zahl und Komplexität der Angriffe durch staatliche und privatwirtschaftliche Cyberkriminelle ist die weltweite Knappheit an Cybersicherheitsexperten in vielen Unternehmen und Organisationen schon heute schmerzlich spürbar.

Es hapert jedoch nicht nur daran, dass die Fachkräfte im Bereich Cyber Security schlicht und einfach fehlen, sondern auch daran, dass einige Security-Experten ihren Beruf nicht mehr ausüben möchten. So zeigen zahlreiche Studien, dass viele Mitarbeitende im Bereich Cyber Security mit dem Gedanken spielen, den Job zu wechseln.

Wie wird sich die Herausforderung weiterentwickeln?

«Infolge geopolitischer Spannungen und makroökonomischer Instabilität sowie öffentlichkeitswirksamer Datenschutzverletzungen und wachsender Herausforderungen im Bereich der physischen Sicherheit rückt das Thema Cybersicherheit stärker in den Mittelpunkt und die Nachfrage nach Fachkräften in diesem Bereich steigt», so Clar Rosso, CEO von (ISC)² – dem International Information System Security Certification Consortium.

Viele Unternehmen setzen auf Trainingsplattformen für Cyberspezialisten, um die innerbetriebliche Aus- und Weiterbildung gezielt zu stärken. Allerdings mangelt es oft an einer sinnvollen Integration in die Aus- und Weiterbildung von Mitarbeitenden, die in ihren Entwicklungs-, Betriebs- und Innovationsprozessen zunehmend Security Skills benötigen. Fragen wie «Wie gestalte ich das Training und die Weiterbildung so attraktiv, dass sie von den Tech-Mitarbeitenden angenommen und auch begleitend zum ‹Daily Business› eingesetzt werden?» oder «Welche Möglichkeiten ergeben sich dadurch auch für eine aktive Trainingskampagne im Spezialistenumfeld?» bleiben häufig unbeantwortet. Zum eigentlichen Trainingsangebot gesellt sich dann auch schnell die Frage nach dem richtigen organisatorischen Setting.

Heute wird von Bewerberinnen und Bewerbern immer wieder bemängelt, dass sie im Rekrutierungsprozess als Mensch zu wenig im Zentrum stehen: lange Reaktionszeiten aufseiten der Unternehmen auf Bewerbungen, starre Regelungen und festgefahrene Lohnbänder, fehlende Transparenz im Rekrutierungsprozess u.v.m. werden als negative Beispiele genannt. Dies lässt bei manch einem der kritisierten Unternehmen auf unprofessionelle Rekrutierungsprozesse schliessen. Um als nachhaltig attraktiver Arbeitgeber für Cybertalente wahrgenommen zu werden, ist eine stringente Employer Journey im Rekrutierungsprozess erstrebenswert.

Wie kann man der Herausforderung wirkungsvoll begegnen?

Arbeitsbedingungen verbessern: Geld allein macht nicht glücklich – ist aber durchaus ein entscheidender Faktor. Abgesehen von der angemessenen Entlöhnung können Firmen auch in Sachen Arbeitsumfeld und Vereinbarkeit von Beruf und Familie punkten. Die Möglichkeiten sind hier vielfältig: flexible Arbeitszeiten, Homeoffice-Modelle, reduzierte Arbeitszeit bei gleichem Gehalt etc. Welche Optionen für einen Betrieb realistisch sind, müssen Unternehmen selbst analysieren und entscheiden.

Erwartungen an Bewerbende anpassen: Einsteiger- bzw. Junior-Positionen mit Studienabschluss und mindestens fünf Jahren Berufserfahrung entsprechen nicht der Realität. Hier sollte manch ein Unternehmen die Erwartungen überdenken – ansonsten dürfte sich die Suche nach guten Mitarbeitenden sehr schwierig gestalten.

Weiterbildungen anbieten und intern weiterentwickeln: Durch einschlägige Aus- und Weiterbildungen von berufsbegleitenden Trainings über DevSecOps-Bootcamps bis hin zu Hochschulkursen können sich Mitarbeitende die nötigen Security Skills aneignen und so neue Aufgaben übernehmen. Damit das eigene Personal diese Möglichkeit nutzt, müssen Unternehmen entsprechende Anreize schaffen, z.B. durch eine Beteiligung an den Weiterbildungskosten.

Outsourcing einsetzen und Arbeitspensum reduzieren: Um das Arbeitspensum in der Security zu senken, lassen sich bestimmte Aufgabenbereiche an externe und spezialisierte Dienstleister auslagern. Externe Dienstleister können dabei helfen, spezifische Lücken im unternehmenseigenen Know-how zu schliessen (Knowledge Gap).

«Wir müssen dringend die Talentlücke im Bereich der Cybersicherheit schliessen. Um dies zu erreichen, müssen wir Zugangsbarrieren abbauen, Menschen mit sinnstiftender Arbeit im Bereich der Cybersicherheit an die Organisation binden und sicherstellen, dass die Mitarbeitenden auch langfristig bleiben. Auch eine zielgruppengerechte Ausbildung im internen DevSecOp-Umfeld unterstützt proaktiv den ‹Kampf um Talente›.»

Marcus Beyer
Security Awareness Officer

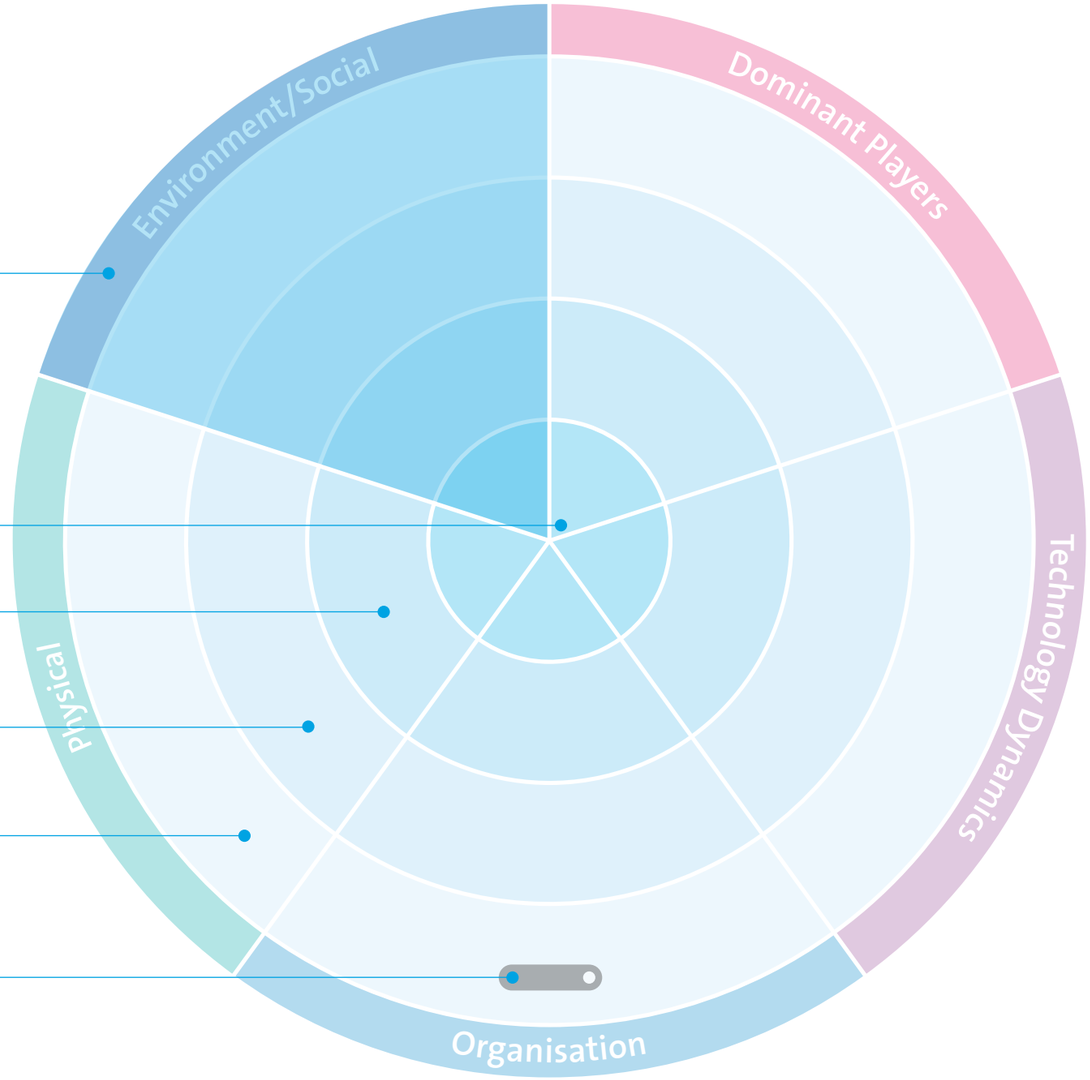
Methodik

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

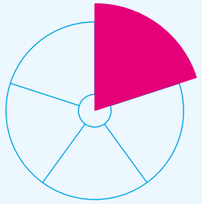
Die Kreise kennzeichnen wir als:

- **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.
- **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.
- **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** 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.

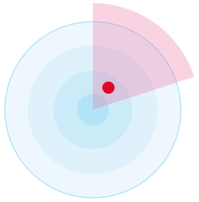


Details inkl. Tendenzen und Vergleich zum Vorjahr



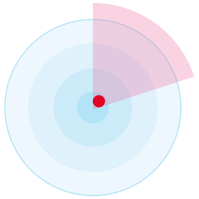
Dominant Players

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



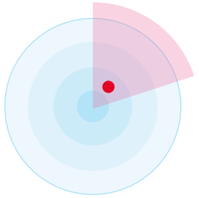
Concentration Data & Cloud Services
Die starke Zentralisierung von Daten in der Cloud führt zu Klumpenrisiken. Der Ausfall eines Service oder zentralen Dienstes kann weltweit Auswirkungen haben.

▲ Zunehmend



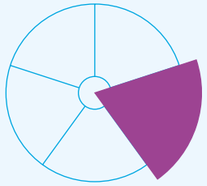
Infrastructure Integrity
In wesentliche Komponenten kritischer Infrastrukturen können fahrlässig oder bewusst Schwachstellen eingebaut worden sein, welche die Systemsicherheit gefährden.

► Unverändert



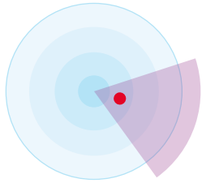
Legacy Protocols
Durch Softwareabhängigkeiten werden immer noch völlig veraltete, angreifbare Protokolle verwendet (z.B. NTLMv1, SMBv1, RC4), wodurch einige wenige Applikationen die Sicherheit ganzer Infrastrukturen gefährden.

► Unverändert



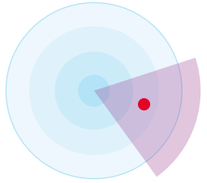
Technology Dynamics

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.



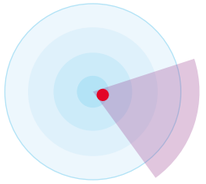
5G Security
5G ist eine noch junge Mobilfunktechnologie. Die Einführung wird neben vielen Chancen auch noch unbekannte Bedrohungen mit sich bringen.

► Unverändert



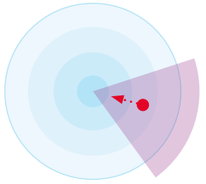
Quantum Computing
Quantencomputer können bestehende kryptografische Verfahren unbrauchbar machen, da sie diese in kürzester Zeit umgehen können.

▼ Abnehmend



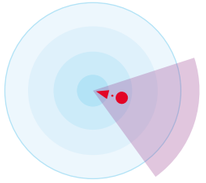
Ransomware
Kritische Daten werden grossflächig verschlüsselt und gegen Lösegeld (möglicherweise) wieder entschlüsselt.

▲ Zunehmend



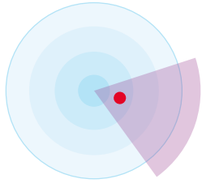
Increased Complexity
Die Komplexität von Systemen, insbesondere über Technologie- und Unternehmensgrenzen hinweg, nimmt laufend zu. Gerade im Hybrid-/Multi-Cloud-Umfeld mit vielen Cloud-Anbietern werden IT-Landschaften komplexer. Dadurch steigt die Risikoexposition und die Fehlersuche wird erschwert.

▲ Zunehmend



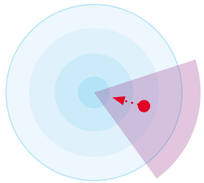
AI-Based Attacks
Angriffe mittels künstlicher Intelligenz (KI) sind gezielter und dadurch schwerer erkennbar. Durch KI können Angriffe effizienter auf klassische Angriffsvektoren wie Ransomware, Phishing, Spear-Phishing und vereinzelt auch auf neue Szenarien wie Deep Fakes, Desinformation u.Ä. durchgeführt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

▲ Zunehmend



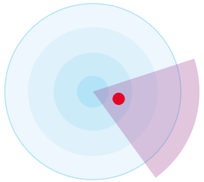
Targeted Attacks
Gezielte und komplexe Angriffe, um ein konkretes Ziel zu erreichen. Schlüsselpersonen werden identifiziert und gezielt direkt oder indirekt (Lateral Movement, Social-Engineering-Methoden) angegriffen, um dadurch relevante Informationen zu erhalten oder maximalen Schaden anzurichten.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

► Unverändert



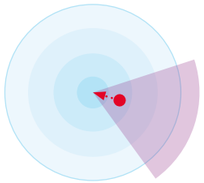
DDoS Attacks
Ein Denial-of-Service-(DDos-)Angriff ist ein böswilliger Versuch, den normalen Datenverkehr eines Zielservers, -dienstes oder -netzwerks zu stören, indem das Ziel oder die umgebende Infrastruktur mit einer Flut von Internetverkehr überschwemmt wird. DDoS-Angriffe erreichen ihre Effektivität,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



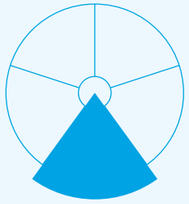
Supply Chain Attacks
Angriffe auf die Lieferkette zielen auf die Ausnutzung von Vertrauens- und Geschäftsbeziehungen zwischen einem Unternehmen und externen Parteien ab. Zu diesen Beziehungen können Partnerschaften, Lieferantenbeziehungen oder die Verwendung von Software Dritter gehören.

▲ Zunehmend



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.

▲ Zunehmend



Organisation

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

Workplace Heterogeneity
Neben den vielen Chancen, die neue Arbeitsmodelle mit sich bringen, führt der unkontrollierte Einsatz solcher Modelle, 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

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

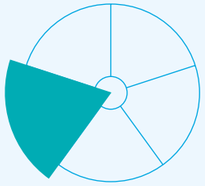
► Unverändert

Security Skills
Durch die Komplexität der Cyberangriffe und die voranschreitende Digitalisierung werden Security Skills und der Einsatz von Cyber Professionals in der Organisation unabdingbar. Ein drohender «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.

▲ 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.

▲ 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.

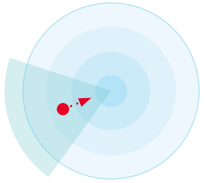
▼ Abnehmend

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

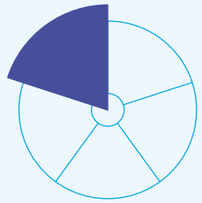
Unsecure IoT/OT Devices
Ob Betriebstechnologie (OT) zur Überwachung und Steuerung von physischen Prozessen, Geräten und Infrastrukturen, oder IoT-Geräte – das Internet der Dinge ist immer und überall. Dabei werden hier verschiedenste Aufgaben – von simpel bis komplex – erfüllt, die von Home-Entertainment-Anwendungen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

► Unverändert



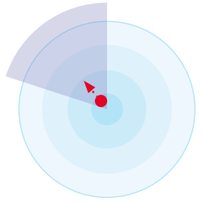
Targeted Sabotage
Es geht um die gezielten Attacken auf wichtige kritische Infrastrukturen, Versorgungsanlagen und Leitungen, was zu beachtlichen Einschränkungen im Internet führen kann. Die gezielte Sabotage von neuralgischen Glasfaserkabeln nimmt zu, ist eine Gefahr und muss beobachtet werden. Gegenmassnahmen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

▲ Zunehmend



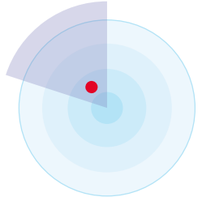
Environment/Social

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



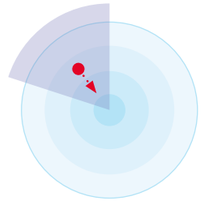
Security Job Market
Der Bedarf an Security Professionals ist enorm gross und kann nur sehr schwer gedeckt werden. Dies führt zu einem abnehmenden Know-how im Kampf gegen immer komplexere und intelligentere Angriffe.

► Unverändert



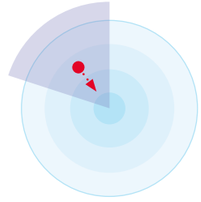
Digital Identity
Beglaubigte, persönliche digitale Identitäten können missbraucht oder gestohlen werden, um z.B. unter fremdem Namen Verträge abzuschliessen.

▲ Zunehmend



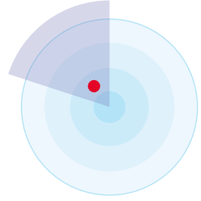
Disinformation & Destabilisation
Die absichtliche Verbreitung von unwahren Informationen kann zu einer wirtschaftlichen und gesellschaftlichen Destabilisierung führen und wird gerade in Krisenszenarien vermehrt auch über den Cyberraum gezielt eingesetzt.

▲ 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

Fazit

Security by Design als konsequente Berücksichtigung und Integration von Sicherheitsaspekten in allen Phasen der Softwareentwicklung – also von der Idee bis zur Einführung und Nutzung der Produkte – wird nicht nur immer wichtiger, sondern bildet das Rückgrat für eine stabile Cybersicherheit von Unternehmen und Organisationen.

In Kombination mit einem Human-Centered-Security-Ansatz, also der konsequenten Sensibilisierung der Mitarbeitenden in Sicherheitsbelangen, werden Unternehmen sicherer und sind auf drohende Krisensituationen vorbereitet.

Wer sich die Zeit nimmt, um mögliche Risiken zu identifizieren, wird schnell feststellen, dass es allerlei denkbare Krisenszenarien gibt, welche das eigene Unternehmen in Schieflage bringen könnten. Diesen Gefahren müssen thematisiert und analysiert werden. Den Kopf in den Sand zu stecken, ist sicherlich keine nachhaltige Option und nicht zu empfehlen.

Die Auseinandersetzung mit Cyberrisiken ist fordernd. Dabei ist es aber immens wichtig, das Risikodispositiv im Blick zu behalten und sich generell der Cybersicherheitsrisiken bewusst zu sein – und auch der damit einhergehenden Ausfallrisiken.

Wenn also bestehende Denkmuster, Konzepte und Technologien keine befriedigenden Antworten mehr liefern, müssen neue Denkansätze, Vorgehensweisen, Rollen und Technologien ausprobiert, eingeführt und etabliert werden. Und das erfordert eine gut durchdachte Vision, eine Strategie, Mut und jede Menge Ausdauer.

Für Unternehmen bedeutet diese Investition in die Zukunft also eine riesige Herausforderung. Gerade das Über- und Neudenken von bestehenden Denkmustern und Prozessen innerhalb der IT-Abteilungen gestaltet sich oft als sehr schwierig und ist mit viel Aufwand und Geduld verbunden. Doch genau solche Veränderungen sind manchmal bitter nötig, um das eigene Unternehmen vor Bedrohungen zu schützen. Denn ausser Frage steht, dass sich die Cyberrisiken im Schnellzugtempo weiterentwickeln. Nur Unternehmen, die Schritt halten und über eine agile Security verfügen, werden auch künftig angemessen vor Cyberkriminalität geschützt sein.

«Das Zusammenspiel von Menschen, Prozessen und Technologien bildet das Fundament, um damit eine unternehmerische Resilienz und Stabilität in unsicheren Zeiten zu schaffen.»

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 2023 by Swisscom (Schweiz) AG, Group Security, Alte Tiefenaustrasse 6, 3048 Worblaufen, swisscom.ch
Druck	OK DIGITALDRUCK AG, Zürich
Auflage	200 Exemplare

Swisscom geht voran und gestaltet Innovationen so, dass die Menschen darauf bauen und vertrauen können. Als «Innovators of Trust».

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

Mehr zu unseren Produkten, Dienstleistungen und dem Engagement für Sicherheit in der Schweiz findest du unter swisscom.ch/de/about/sicherheit.html

#BeTheStrongestLink