swisscom

Cyber Security Threat Radar
2020/2021

Unternehmerische Resilienz und Agilität sind gefordert

Inhalt

Cyber Security Threat Radar 04

Lagebild – Bedrohungsradar 06

Methodik 08

Details inkl. Trend und Vergleich zum Vorjahr 10

Herausforderungen und Trends 22

Fazit 26

Impressum

Herausgeberin	Swisscom AG, Group Security
Konzept / Realisation	Agentur Nordjungs, Zürich
Redaktion	Swisscom AG, Group Security
Copyright	© April 2021 by Swisscom (Schweiz) AG, Group Security, Alte Tiefenaustrasse 6, 3048 Worblaufen, swisscom.ch
Druck	OK DIGITALDRUCK AG, Zürich
Auflage	125 Exemplare

«Besondere Lagen erfordern besondere Massnahmen im Umfeld von Sicherheit, Schutz und Risikobewusstsein.»

Philippe Vuilleumier
Head of Group Security
Swisscom (Schweiz) AG

Cyber Security Threat Radar

Gerade in einer disruptiven, besonderen Lage – wie sie zurzeit herrscht – ist es wichtig, den Überblick zu behalten. Viele Menschen fragen sich, ob die Corona-Pandemie mehr Cyberaktivitäten hervorgerufen hat. Sind wir mit Homeoffice, Social Distancing und gewissen Unsicherheiten angreifbarer geworden? Unsere Antwort lautet: **JEIN.**

Besondere Lagen erfordern besondere Massnahmen im Umfeld von Sicherheit, Schutz und Risikobewusstsein. Und ja, die Auslagerung der gesamten IT-Infrastruktur in die Heimbüros der Mitarbeitenden stellte viele Unternehmen und Organisationen vor teilweise schwierige Herausforderungen.

Aber führt die derzeitige Situation zu mehr Angriffen? Besteht ein gesteigertes Potenzial an Angriffsvektoren? Das können wir so nicht bestätigen. Unsere Experten in den verschiedenen Security Operation Centern der Swisscom überwachen die gesamte Netzinfrastruktur der Schweiz und konnten weder ein verstärktes Angriffsverhalten noch vermehrte Phishing- oder Ransomware-Wellen feststellen.

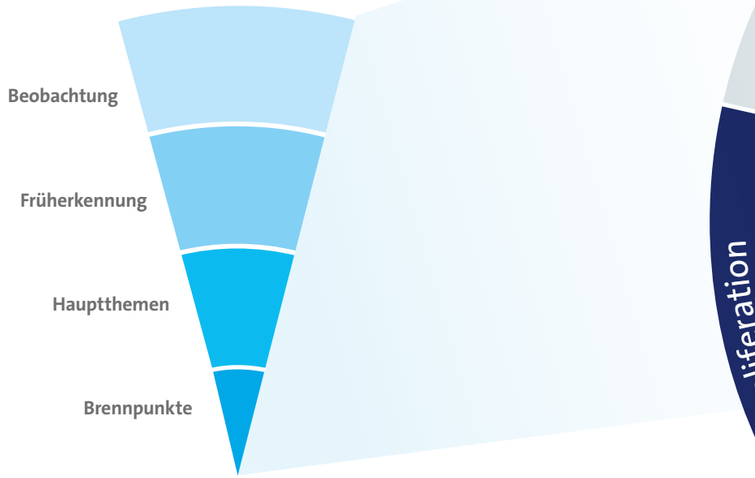
Doch was ist an den Berichten dran, dass Schweizer Kliniken vermehrt angegriffen werden? Was ist mit den in den Medien gemeldeten Cybervorfällen bei mehreren Schweizer Unternehmen? Die gab es auch 2020 – aber Corona-bedingt? Sicher nicht. Organisatorische, prozessuale oder technische Schwächen lagen bereits vor der besonderen Lage vor. Und ja, auch Swisscom war 2020 vor Netzausfällen nicht verschont geblieben. Die Störungen konnten schnell behoben werden – aber ein fahler Beigeschmack ist zurückgeblieben. Für viele Unternehmen und Organisationen geht es darum, Schwächen auszumerzen, sie in Stärken umzuwandeln und eine Sicherheitskultur aufzubauen, die technische, organisatorische wie auch prozessuale Änderungen schafft, um resilient in die Zukunft schauen zu können.

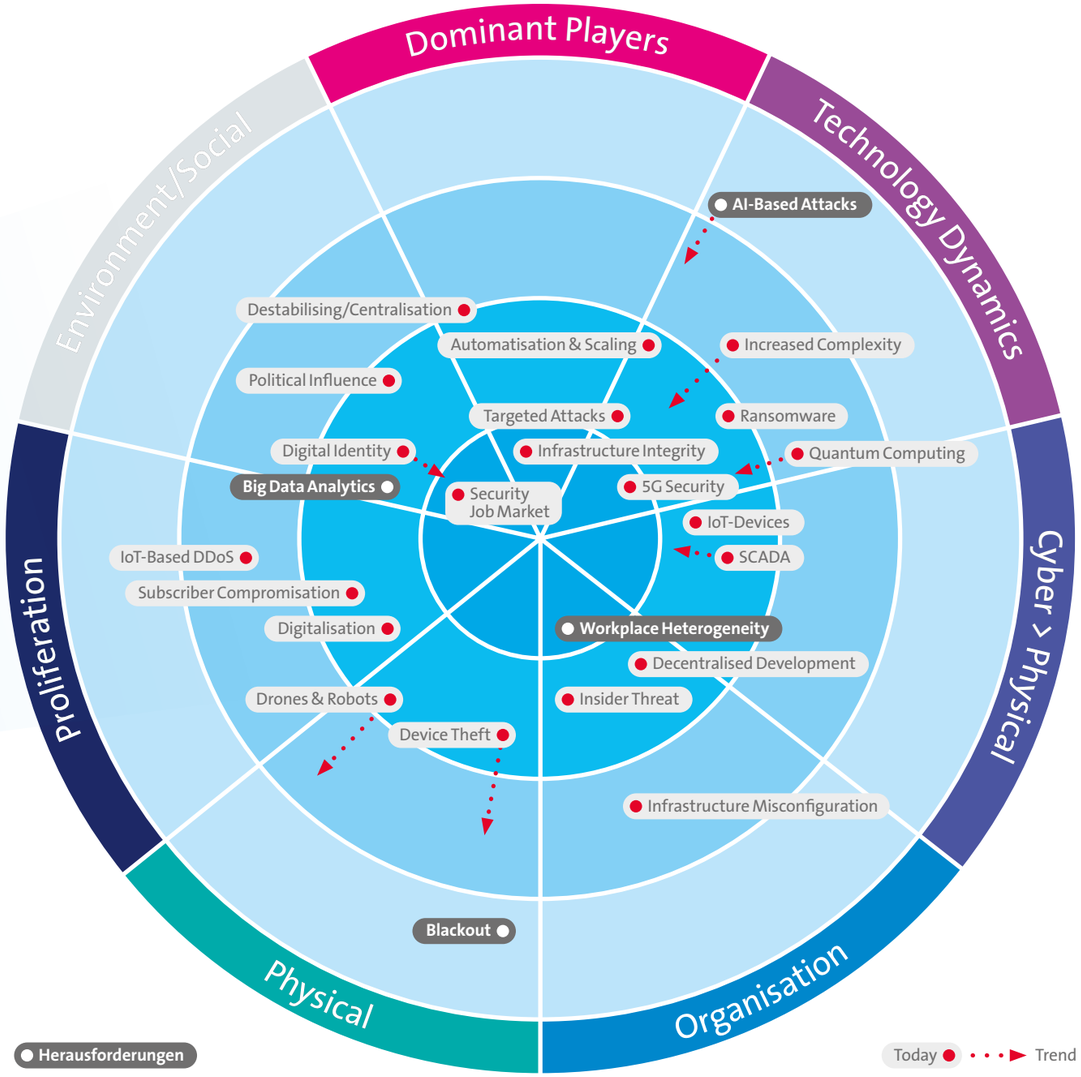
Mit dem vorliegenden Cyber Security Threat Radar 2020/2021 wurde die aktuelle Bedrohungslage ermittelt, um einen Überblick über drohende Cyberrisiken und das von ihnen ausgehende Gefahrenpotenzial zu erhalten. Er betrachtet und beobachtet Trends, wie auch Herausforderungen, bewertet diese und verschafft durch das Bündeln von Expertenwissen einen Überblick über die Bedrohungslage und deren Entwicklung in der Schweiz. Er beschreibt die Motivation und die Mittel der Angreifer. Basierend auf den von Swisscom gesammelten und ausgewerteten Daten zeigt er auf, welche Methoden und Werkzeuge Angreifer am häufigsten verwenden. Zudem erklärt er, welche Gegenmassnahmen besonders effektiv sind, um einen Angriff bestmöglich erkennen zu können. Der Cyber Security Threat Radar 2020/2021 dient als Leitfaden und Kompass, um sicher durch die Cyberwelt zu manövrieren.

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, auf den wir auch schon in früheren Publikationen des Swisscom Security Report verwiesen haben.





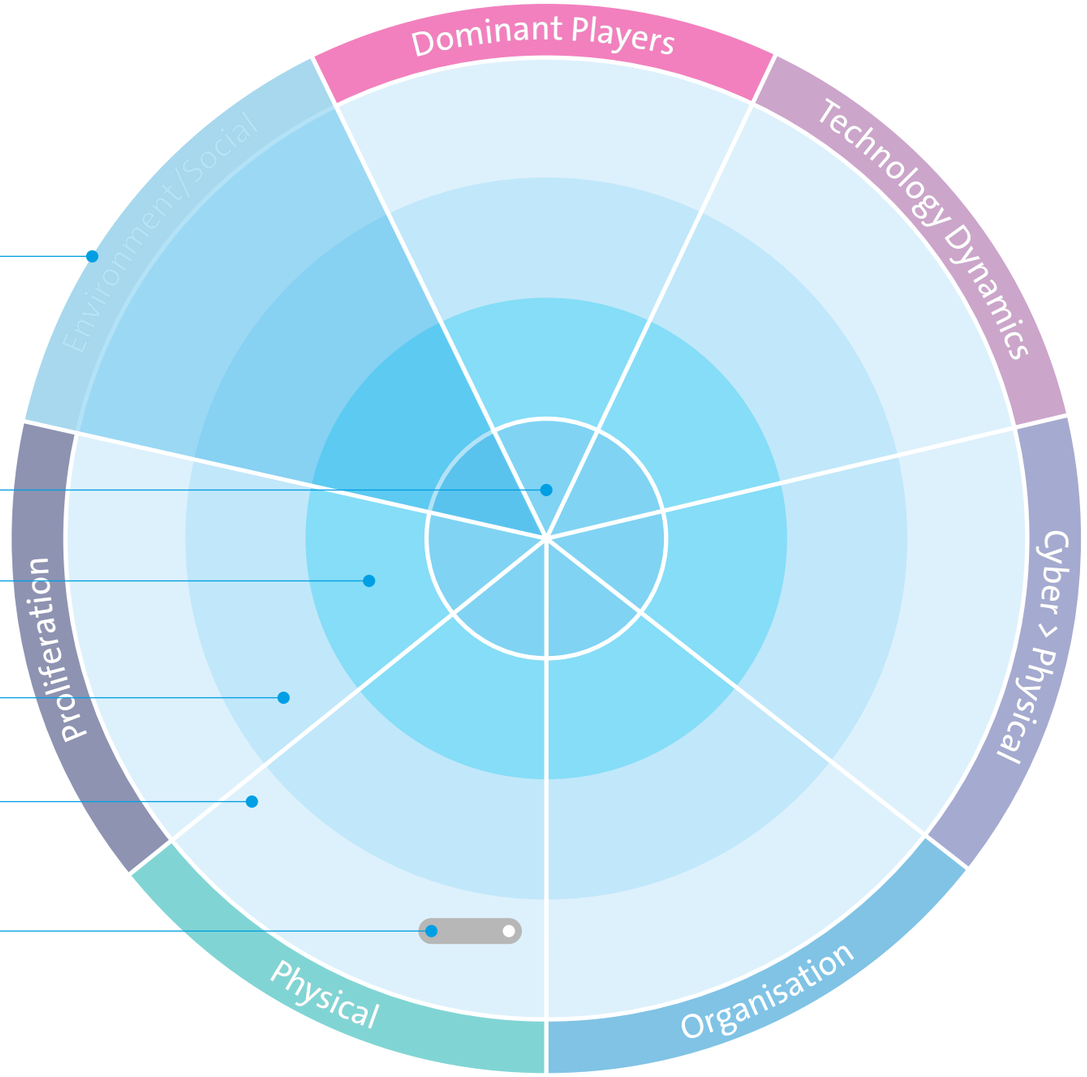
Methodik

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

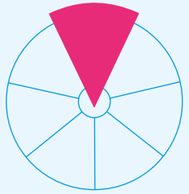
Die Kreise kennzeichnen wir als:

- **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 wenig Wirkung zeigen. 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.

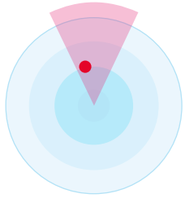


Details inkl. Trend und Vergleich zum Vorjahr



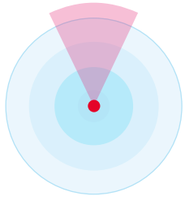
Dominant Players

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



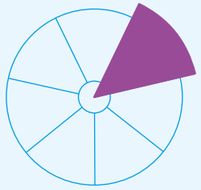
Destabilising/Centralisation
Starke Zentralisierung in der Struktur des Internets führt zu Klumpenrisiken. Der Ausfall eines Service kann weltweit Auswirkungen haben, wie zum Beispiel ein Ausfall von Amazon Web Services (AWS).

► Unverändert



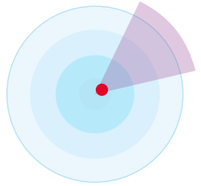
Infrastructure Integrity
In wesentliche Komponenten kritischer Infrastrukturen können fahrlässig oder bewusst Schwachstellen eingebaut worden sein, welche die Systemsicherheit gefährden.

► Unverändert



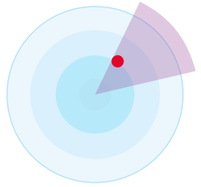
Technology Dynamics

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 Entwicklung selber neue Bedrohungen schaffen.



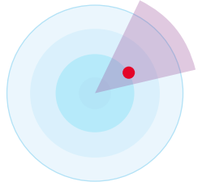
5G Security
5G ist eine noch junge Mobilfunk-Technologie. Die Einführung wird neben vielen Chancen auch noch unbekannte Bedrohungen mit sich bringen.

▲ Zunehmende Bedrohung



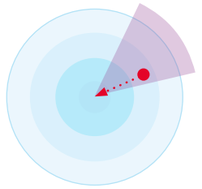
Automatisation & Scaling
Die stärkere Automatisierung technischer Betriebsprozesse wird bei erfolgreichen Angriffen oder Fehlkonfigurationen grössere Auswirkungen haben.

▲ Zunehmende Bedrohung



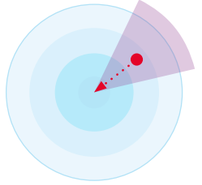
Ransomware
Kritische Daten werden grossflächig verschlüsselt und gegen Lösegeld (möglicherweise) wieder entschlüsselt.

▼ Abnehmende Bedrohung



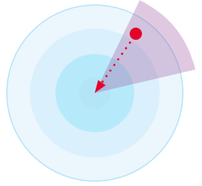
Quantum Computing
Quantencomputer können bestehende kryptografische Verfahren unbrauchbar machen, da sie diese in kürzester Zeit knacken können.

► Unverändert



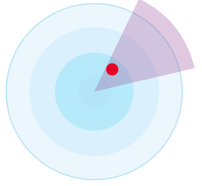
Increased Complexity
Die Komplexität von Systemen, insbesondere über Technologie- und Unternehmensgrenzen hinweg, nimmt laufend zu. Dadurch steigt die Risikoexposition und die Fehlersuche wird erschwert.

► Unverändert



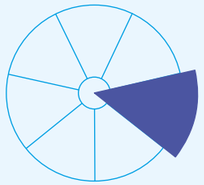
AI-Based Attacks
Angriffe mittels künstlicher Intelligenz (KI) sind gezielter und dadurch schwerer erkennbar. Durch KI können Angriffe effizienter auf klassische Angriffsvektoren wie z.B. Ransomware, Phishing, Spear-Phishing und vereinzelt auch auf neue Szenarien, wie z.B. Deepfakes, Desinformation u.ä.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

▲ Zunehmende Bedrohung



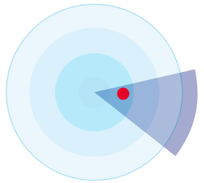
Targeted Attacks (APTs)
Gezielte und komplexe Angriffe, um ein konkretes Ziel zu erreichen. Schlüsselpersonen werden identifiziert und gezielt direkt oder indirekt (lateral movement) angegriffen, um relevante Informationen zu erhalten oder maximalen Schaden anzurichten. Ein wesentlicher Aspekt ist die Persistenz, d.h., dass die Angreifer möglichst lange unentdeckt agieren.

► Unverändert



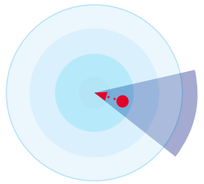
Cyber > Physical

Unter diesen Begriff fallen Angriffe über die Infrastruktur im Cyberspace, die vermehrt Schaden in der physischen Welt verursachen werden.



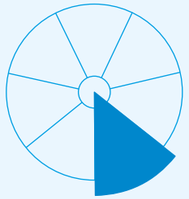
IoT-Devices
Schwach geschützte Geräte können kompromittiert und sabotiert werden. So können sie in der eigenen Funktion, z.B. der Verfügbarkeit oder Datenintegrität, eingeschränkt werden.

- Unverändert



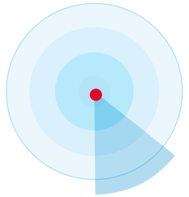
SCADA
Es existieren nach wie vor viele schlecht oder gar nicht geschützte Kontrollsysteme für Anlagen der kritischen Infrastruktur.

- Unverändert



Organisation

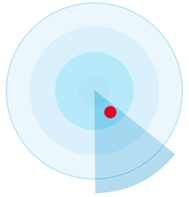
Unter Organisation sind Bedrohungen zu verstehen, die von Veränderungen in Organisationen ausgehen oder Schwächen in Organisationen ausnutzen.



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.

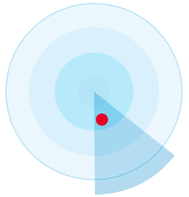
▲ Zunehmende Bedrohung



Decentralised Development

Klassische Entwicklungsabteilungen sterben aus und die Applikationsentwicklung rückt näher in die Business Units bei gleichzeitig kürzer werdenden Release-Zyklen.

► Unverändert



Insider Threat

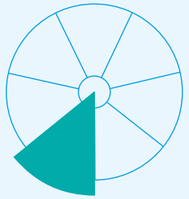
Partner oder Mitarbeitende manipulieren, missbrauchen oder verkaufen Informationen fahrlässig oder vorsätzlich.

▲ Zunehmende Bedrohung

Infrastructure Misconfiguration

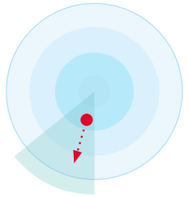
Ausnutzung von fehlkonfigurierten Infrastrukturkomponenten und/oder von Schwachstellen, die spät identifiziert und behoben werden.

▼ Abnehmende Bedrohung



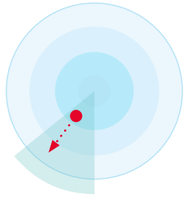
Physical

Bedrohungen, die von der physischen Umgebung ausgehen und in der Regel eher auf physische Ziele ausgerichtet sind.



Device Theft
Der Diebstahl, insbesondere von Komponenten der kritischen Infrastruktur oder künftig vermehrt von IoT-Geräten, kann zum Datenverlust führen oder die Verfügbarkeit der Services beeinträchtigen.

► Unverändert

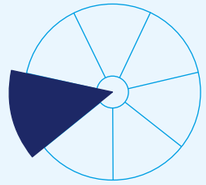


Drones & Robots
Aufklärung oder Angriffe über weite Entfernungen werden einfacher und günstiger. Miniaturisierung führt zu schlechter Erkennbarkeit der Angreifer.

► Unverändert

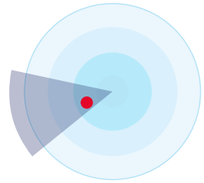
Blackout
Angriffe auf kritische Infrastrukturen wie Stromnetzbetreiber. Ausfallsicherheit ist essenziell und Business Continuity wird verstärkt auch in der Cyber-Resilienz-Debatte thematisiert.

▲ Zunehmende Bedrohung



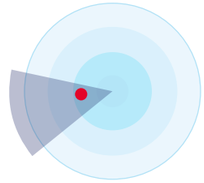
Proliferation

Bedrohungen, die von der immer einfacheren und günstigeren Verfügbarkeit von IT-Medien und Know-how profitieren, fallen unter das Segment Proliferation. Einerseits, weil die Verbreitung zu mehr Angriffsflächen führt und andererseits, weil sie die Verfügbarkeit von Angriffswerkzeugen erhöht.



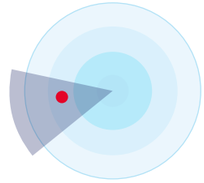
Digitalisation
Immer stärkere Vernetzung der realen und der virtuellen Welt im Privat- und im Geschäftsleben führt zu mehr Angriffswegen.

► Unverändert



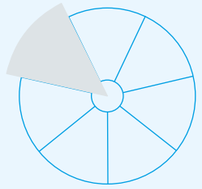
Subscriber Compromisation
Schadsoftware greift private Daten der Mobilenutzer an oder wird für Angriffe auf die Telekommunikations- bzw. IT-Infrastruktur genutzt.

► Unverändert



IoT-Based DDoS
Starkes Wachstum bei geringem Schutz von IoT-Geräten führt zu mehr «Übernahmekandidaten» für Botnetze.

► Unverändert

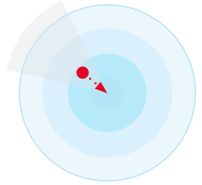


Environment/Social

Damit sind Bedrohungen gemeint, die von gesellschaftlich-politischen Änderungen ausgehen oder durch solche Änderungen für Angreifer einfacher oder wertvoller werden.

Security Job Market
Der Bedarf an Security-Professionals kann nur sehr schwer gedeckt werden, was weniger Know-how im Einsatz gegen immer komplexere und intelligentere Angriffe zur Folge hat.

► Unverändert



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

► Unverändert

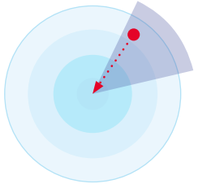
Big Data Analytics
Mehr Daten und bessere Analysemodelle können missbraucht werden, um das Verhalten von Menschen zu beeinflussen. Entscheidungen werden vermehrt autonomen Systemen überlassen. Der Missbrauch von Daten aus «Big Data Lakes» wird gezielt für Desinformation, Fake News, gesellschaftliche und psychosoziale Analysen sowie die Erstellung von Bewegungsmustern herangezogen. Damit geht eine Verletzung der Privatsphäre einher.

▲ Zunehmende Bedrohung

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

Herausforderungen und Trends



AI-Based Attacks

Worum gehts?

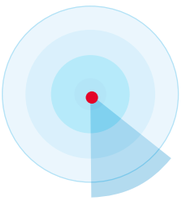
Die letzten Jahre waren immer wieder von Datenschutz- und Sicherheitsverletzungen überschattet. Aber auch das Thema «Deepfakes» oder «Desinformation im Allgemeinen» stand im Fokus.

Wie wird es sich entwickeln?

Künstliche Intelligenz wird von Tag zu Tag stärker, erweitert die eigenen Fähigkeiten und lernt permanent hinzu. Und die Vor- und Nachteile dieser Technologie standen schon immer im Rampenlicht – gekommen, um zu bleiben.

Wie kann man der Herausforderung / dem Trend wirkungsvoll begegnen?

- Das Training und die Sensibilisierung der Mitarbeitenden hat hier höchste Priorität
- Technische Vorsorge mittels SOC zur Analyse und Identifikation solcher Angriffe



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 – jetzt durch die Pandemie getrieben – verstärkte Einsatz von Remote-Arbeitsplätzen, zu einer grösseren Risikoexposition.

Stärkste Änderung im Radar seit 2020 und in den Brennpunkt gerutscht – natürlich schon fast disruptiv getrieben durch die Pandemiesituation weltweit. Der «New Work» und das Arbeiten im Homeoffice wird sich sicher auch nach der Pandemie verstärkt in den Unternehmen verankern und zu einem akzeptierten Arbeitsmodell werden.

- Anpassung bestehender Policies und Weisungen; weg vom «Telearbeitsplatz» hin zu Mobile Working
- Sicherheitsstandards wie Privileged Access Management integrieren
- Risikomanagement auf den mobilen Workplace erweitern und agiles Risikomanagement vorantreiben
- Multifaktor-Authentifizierung stärken und in die Systemlandschaft integrieren
- Etablierung einer konsequenten Sicherheitskultur unter Einbezug der Mitarbeitenden (human-centered approach)

Blackout

Worum gehts?

Angriffe auf kritische Infrastrukturen wie Stromnetzbetreiber. Die Medien zeigen, dass die Verwundbarkeit kritischer Infrastrukturen durch Cyberangriffe stark zugenommen hat. Ausfallsicherheit wird ein wichtiges Element und Business Continuity wird verstärkt auch in der Cyber-Resilienz-Debatte thematisiert.

Wie wird es sich entwickeln?

Die Angriffe auf kritische Infrastrukturen werden definitiv weiter zunehmen und sich verstärken. Wir spüren hier zudem ein hohes Risiko durch ein altersbedingtes Ausscheiden von Schlüsselpersonen im Betrieb von SCADA-Systemen sowie eine wachsende Komplexität von IoT-Devices auf den Betreiberplattformen.

Wie kann man der Herausforderung / dem Trend wirkungsvoll begegnen?

- Business Continuity Management sollte eine stärkere Beachtung in der Planung von Cybersicherheitsstrategien erhalten
- Kollaboratives und interdisziplinäres Agieren in Unternehmen und Organisationen
- DevSecOps – Frameworks in agilen Settings aufsetzen und aktiv unterstützen
- Verantwortung in der «First Line of Defense» stärken

Big Data Analytics

Mehr Daten und bessere Analysemodelle können missbraucht werden, um das Verhalten von Menschen im Umgang mit Daten und IT-Systemen zu beeinflussen. Entscheidungen werden vermehrt autonomen Systemen überlassen. Der Missbrauch von Daten aus «Big Data Lakes» wird gezielt für Desinformation, Fake News, gesellschaftliche und psychosoziale Analysen herangezogen. Damit geht eine Verletzung der Privatsphäre einher, die gesellschaftliche Auswirkungen haben kann.

Daten sind das neue Gold – zumindest titelt so sehr häufig die Wissenschaft und die Fachpresse. Demgegenüber steht der Nutzen für die Berechnung komplexer gesellschaftlicher Systeme und die Verfügbarkeit von Daten zu Analysezwecken, zum Beispiel im Gesundheitssektor. Hier gibt es viel Spielraum für neue Entwicklungen, aber auch das Risiko des «gläsernen Bürgers» bzw. der massive Abfluss von sensiblen (Unternehmens-)Daten. Die Korrelation von verfügbaren und durchsuchbaren Daten, z.B. via OSINT, öffnet auch Cyberkriminellen und Social Engineers Tür und Tor.

- Ethische Leit- und Grundsätze sind hier besonders wichtig – auch in der Nutzung der einem anvertrauten Daten
- Technische sowie organisatorische Einschränkung von Zugriffen auf die Daten ist notwendig
- Sensibilität entwickeln: Mit welchen Cloud-Services gehe ich wie um? Welche Daten werden wo abgelegt?

Fazit

2020 war ein disruptives und herausforderndes Jahr für Organisationen und Unternehmen, für Mitarbeitende wie auch für die Schweizer Sicherheitsabteilungen. Es war ein Jahr, das neben den ganzen Hürden und Einschränkungen aber auch die Chance für neue Entwicklungen und Perspektiven geboten hat.

Kein Wunder also, dass das Thema Workplace Heterogeneity in den Brennpunkt des diesjährigen Cyber Security Threat Radar gerutscht ist – sicherlich eine der grössten Veränderungen eines Threat Vectors in den vergangenen Jahren. Die sofortige Entsendung aller Mitarbeitenden ins Homeoffice war eine der intensivsten Herausforderungen, die Sicherheits- und IT-Abteilungen in jüngster Vergangenheit bewerkstelligen mussten. Und es hat funktioniert – manchmal gut, manchmal weniger. Aber insgesamt ist es gut gelungen. Dies zeigt deutlich, wie agil Unternehmen und Organisationen in der heutigen Welt agieren müssen, um mit dem Wettbewerb, dem Markt und den gesellschaftlichen Anforderungen Schritt halten zu können.

In vielen Unternehmen und Organisationen hat die digitale Transformation einen heftigen Schub vorwärts gemacht. Die grossen Innovationen fehlen aber, wirklich Neues wurde nicht entwickelt. Dafür haben schon bestehende Werkzeuge stärker Einzug in den «New Way of Working» gehalten. Die Sicherheitsanstrengungen von Zoom (vom Zoom-Bombing zur End-to-End-verschlüsselten Kommunikation) und die Weiterentwicklung von Microsoft Office 365 als kollaboratives Tool sind spürbar und sichtbar. Der digitale Wandel entwickelt sich rasant weiter – oft auch auf Kosten der Sicherheit oder der Privatsphäre und des Datenschutzes, wie die gehypte Audio-Diskussions-App Clubhouse eindrücklich beweist.

> «Der digitale Wandel entwickelt sich rasant weiter, oft auch auf Kosten der Sicherheit oder der Privatsphäre und des Datenschutzes, wie die gehypte Audio-Diskussions-App Clubhouse eindrücklich beweist.»

Big Data spielt auch bei den sozialen Medien, neuen kollaborativen Services und in der Marketing-Maschinerie weiterhin eine grosse Rolle. In Verbindung mit AI-Based Attacks wie Desinformation (Deepfakes, Fake News) bekommt künstliche Intelligenz eine neue Wichtigkeit. Die Angriffsmethoden der Cyberkriminellen werden immer ausgeklügelter und dürften neue Dimensionen erreichen, auf die es sich vorzubereiten gilt.

Dabei kommt der Einhaltung einer konsequenten Sicherheitskultur eine tragende Rolle zu. Die RSA Conference 2020 stellte «The Human Element» in den Fokus – fast schon in Vorahnung auf die besondere Lage, in der wir uns zurzeit befinden. Den Faktor Mensch in den Mittelpunkt zu stellen, auf seine Bedürfnisse, Anforderungen und Probleme gezielt einzugehen, ihn zu schützen und in den zu bewerkstelligenden Sicherheitsprozessen zu unterstützen, rückte 2020 definitiv in den Fokus – und wird uns auch 2021 und darüber hinaus weiter begleiten. Die dynamische Anpassung der Organisation, der Kultur und der Prozesse wird in Hinblick auf die neuen Angriffsvektoren immer wichtiger.

Festzuhalten ist: Die Gefahren in der digitalen Welt wurden nicht weniger. Signifikante Anstiege konnten unsere Experten des Security Operation Center der Swisscom aber nicht feststellen. Sie waren hier und da einfach anders, auf situationsbezogene Themen abgestimmt und fokussierten oft auf den Menschen als Eintrittsvektor. Der Mitarbeitende als «First Line of Defense» ist und bleibt das wichtigste Element in der Sicherheitskette und sollte dementsprechend beachtet werden.

Für eine sicherere vernetzte Welt

Swisscom stellt die Bedürfnisse von Mitarbeitenden, Kunden und Partner ins Zentrum aller Sicherheitsüberlegungen.

Wir entwickeln **sichere Lösungen**, **Produkte und Dienstleistungen** für unsere Kunden und Partner. Um sie zu schützen, nutzen wir **modernste Technologien**, bauen auf unsere **umfassende Infrastruktur** und leben eine konsequente **Sicherheitskultur**.

#talkingaboutsecurity

swisscom.ch/security