STORMSHIELD

MEINUNGEN

WELCHE HERAUSFORDERUNGEN FÜR DIE CYBERSICHERHEIT BIETET DAS JAHR 2023?

Victor Poitevin
Editorial & Digital Manager, Stormshield

Nach Covid-19 als Topthema des Jahres 2021 war das Cyberjahr 2022 von anderen starken Trends geprägt: wirtschaftliche, ökologische und gesellschaftliche Krisen, geopolitische Konflikte oder auch das Aufkommen einer für alle zugänglichen künstlichen Intelligenz ... Gründe genug, um das kommende Jahr zu orientieren. Welches werden die Herausforderungen im Bereich der Cybersicherheit für 2023 sein? Überlegungen zu Aussichten und Trends.

DIE HERAUSFORDERUNGEN BEI DER PERSONALBESCHAFFUNG

Der Markt für Cybersicherheit ist seit mehreren Jahren einem starken Arbeitskräftemangel ausgesetzt. Laut der Studie *Cybersecurity Workforce Study 2022* sind weltweit 3,7 Millionen Stellen zu besetzen.

Die Cybersicherheitsbranche ist in der großen Kündigungswelle nach dem Lockdown gefangen und die Fluktuationsrate steigt rasant an. Laut derselben Studie haben 21 % der Befragten in den letzten 12 Monaten die Stelle gewechselt, was einem Anstieg von 13 % im Vergleich zum Vorjahr entspricht. Gehalt, Arbeitsbedingungen, Unternehmenszweck: All dies sind Elemente, die heute zu gleichen Teilen in die endgültige Entscheidung der Bewerber einfließen.

Ein Mangel, der so weit geht, dass er eine schreckliche Frage aufwirft: **Kann ein Unternehmen für Cybersicherheit wegen Personalmangels zu Grunde gehen?** Bei einigen Dienstleistungsunternehmen im Bereich der Cybersicherheit war das Jahr 2022 ein Test auf Herz und Nieren. Eine Situation, die sich 2023 weiter ausbreiten wird: hin zu einem SOC ohne Ressourcen, das nicht schnell genug auf eine kritische Warnung reagieren kann? Hin zu Unternehmen ohne CISOs?

Doch der Sektor mobilisiert sich und wird aktiv. Während die geopolitische Lage im Jahr 2022 ethische Hackergruppen dazu veranlasst hat, Regierungen zu unterstützen, könnte sich der Trend 2023 fortsetzen. Bis hin zur Strukturierung? Auf der anderen Seite sind die Sensibilisierung in der Schule oder auch die immer zahlreicher werdenden Schulungen zur Cybersicherheit echte Versprechen für die Zukunft. Die Schaffung dieser neuen Talente wirft dann aber weitere Fragen auf: Wie lange wird es dauern, bis sie zur Verfügung stehen? Wird das langfristig verlässlich sein? Zum selben Thema der Personalbeschaffung sollte man mit einem aufmerksamen Auge beobachten, was sich bei Google, Microsoft oder auch Meta abspielt ... **Und wenn die Entlassungswelle in der Tech-Branche eine Chance für die Cyberbranche wäre?** Ebenso wie die Frage, ist auch der Transfermarkt offen.

DIE HERAUSFORDERUNGEN BEI DER ZUSAMMENARBEIT ZWISCHEN ANBIETERN

Mit der zunehmenden Komplexität von Cyberangriffen kann sich ein Cyberanalyst nicht mehr nur auf die Daten stützen, die von der Firewall im Netzwerk oder dem Schutzagenten am Arbeitsplatz gemeldet werden. Er muss einen Überblick darüber haben, was im Informationssystem vor sich geht.

Um ihm bei diesem Überblick zu helfen, muss ein Cybersicherheitsprodukt die Daten, die es produziert und empfängt, aggregieren, korrelieren und klassifizieren. Denn erst die Zusammenführung dieser Datenströme aus verschiedenen Quellen wie Reputationsdatenbanken oder Cyber Threat Intelligence (CTI) ermöglicht die bestmögliche Erkennung der Bedrohung. **Erkennung, Schutz und Abhilfe sind dann die verschiedenen Teile desselben Räderwerks**. Die Cybersicherheit, wie wir sie kannten, entwickelt sich mit der Einführung von Technologien wie EDR, XDR oder auch NDR weiter. Dieser Ansatz kann aber auch mit einer Anhäufung von Cybersicherheitsprodukten in den Unternehmen einhergehen. Für große Unternehmen eine planbare Organisation, für kleinere ein Kopfzerbrechen, ganz zu schweigen von der Budgetfrage. Dies führt dazu, dass der Rationalisierungsbedarf spürbar wird. Aber wie rationalisiert man? Und mit welchen Werkzeugen? Eine Cyberresilienz, die mehr denn je mit dem Konzept der Zusammenarbeit zwischen Anbietern aufgebaut werden muss.

Eine Zusammenarbeit, die nur mit einer gewissen Demut möglich ist, ein Schlagwort, das in der Cyber-Gemeinschaft akzeptiert werden sollte.

DIE HERAUSFORDERUNGEN DER KÜNSTLICHEN INTELLIGENZ

Das ChatGPT-Konversationsmodul, das Ende 2022 eingeführt wurde, hat bereits viel Aufmerksamkeit erregt. Und es wird auch weiterhin für Gesprächsstoff sorgen, wenn es von Cyberkriminellen genutzt wird. ChatGPT wird von einigen als künstliche Intelligenz und von anderen als Konversationsagent vorgestellt. Man muss jedoch zugeben, dass ChatGPT vor allem ausgefeilte Antworten auf fast jede Anfrage ermöglicht.

Anfragen, wie z. B. das Schreiben von Codezeilen. **Reicht das aus, um jeden in einen Cyberkriminellen zu verwandeln?** Vielleicht nicht, denn Skripte können eine Reihe von Fehlern enthalten und sind daher relativ leicht von Schutzlösungen zu erkennen. Aber immerhin ermöglichen sie es unerfahrenen Cyberkriminellen, sich mit dem Thema vertraut zu machen, und anderen, Zeit bei der Code-Kompilierung zu sparen. Parallel dazu kann das ChatGPT-Modul verwendet werden, um überzeugende Texte zu verfassen – und damit *Phishing* in eine neue Ära zu führen ... Zusammen mit den Fortschritten bei Deep Fakes, Video-, Audio- und Sprachsynthesen wird die Offensivfähigkeit der Cyberkriminellen gestärkt. Das geht so weit, dass manche die Entstehung einer echten bösartigen künstlichen Intelligenz prophezeien, ähnlich wie SkyNet in Terminator.

Auf Seiten der Anbieter ist diese Form der künstlichen Intelligenz nicht neu; sie ist bereits seit vielen Jahren in Cybersicherheitslösungen enthalten, wie zum Beispiel auf der Ebene der Verhaltensanalyse. Die Herausforderung wird hier also eher in der Fähigkeit liegen, die Daten zu verarbeiten, um Cyberangriffe zu erkennen. Wer wird es in diesem asymmetrischen Krieg zwischen Anbietern und Cyberkriminellen schaffen, diese neuen Technologien am besten zu beherrschen? Das Rennen ist in vollem Gange ...

DIE ÖKOLOGISCHEN HERAUSFORDERUNGEN

Die Kontrolle des ökologischen Fußabdrucks der Digitalisierung ist ein sensibles Thema. Im Juni 2020 warnte der französische Senat, dass der Sektor für 2 % der Treibhausgase in Frankreich verantwortlich ist (schätzungsweise 4 % auf globaler Ebene, gegenüber 2,6 % bei der Zivilluftfahrt). In jüngerer Zeit warnte die französische Agentur ADEME, dass sich dieser Anteil ohne einen tiefgreifenden Wandel in der digitalen Nutzung bis 2025 weltweit verdoppeln könnte. Und obwohl regelmäßig mit dem Finger auf sie gezeigt wird, spielen hier nicht nur die Streaming-Plattformen eine Rolle.

Die Welt der Cybersicherheit ist nicht für die gesamten 2 % verantwortlich, verursacht aber dennoch einen Teil davon. Da Unternehmen immer mehr Cybersicherheitsprodukte einsetzen, steigt ihr CO2-Fußabdruck mechanisch an, während gleichzeitig große Datenmengen erzeugt werden, die in entfernten Cloud-Umgebungen gespeichert und repliziert werden. Und abgesehen davon,

dass sie Treibhausgase erzeugen, verbrauchen sowohl die Cybersicherheit als auch die IT viel Wasser. Beispielsweise haben die Rechenzentren von Microsoft in den Niederlanden laut der niederländischen Zeitung *Noordhollands Dagblad* im Jahr 2022 nicht weniger als 84 Millionen Liter Wasser verbraucht. Das entspricht dem Jahresverbrauch von 1.750 Bürgern.

Eine der größten technologischen Herausforderungen der Zukunft wird es daher sein, die Effizienz auf dem gleichen Niveau zu halten und gleichzeitig die Cybersicherheitsprodukte zu rationalisieren, die Menge der gesammelten Daten zu reduzieren und den Verbrauch von Hardware-Ressourcen zu verbessern. In Frankreich hat übrigens im Oktober 2022 ein Forschungsprojekt begonnen, um „*die Vorteile digitaler Dienste am Netzrand konkret zu bewerten*". Das Ziel: Die wärmeerzeugende Kapazität von Geräten zu berücksichtigen und sie besser auf Produktionsumgebungen zu verteilen, in denen Wärme benötigt wird. Digitalisierung und Ökologie endlich vereinbar?