Blog

Cyber-Security die wichtigsten -Trends im 2024

Die Cybersecurity-Branche unterliegt einem kontinuierlichen Wandel, geprägt von schnellen und dynamischen Entwicklungen. Trends gehören darum auf den Radar.

Zürich, 19. März 2024 – In einem sich ständig wandelnden Umfeld ist es wichtig, die aktuellen Entwicklungen und Trends im Bereich der Cybersecurity genau zu beobachten, um frühzeitig darauf reagieren zu können. In unserem heutigen Blogbeitrag präsentieren wir die aus unserer Sicht drei zentralen Cybersecurity-Trends für das Jahr 2024 und analysieren die daraus resultierenden Chancen und Herausforderungen für Unternehmen.

Cyber-Security-Trend 1: Künstliche Intelligenz (KI) – Chance und Herausforderung

Die rasante Entwicklung der Künstlichen Intelligenz (KI) hat sie in den letzten Jahren zu einem der meistdiskutierten Themen gemacht, und dieser Trend wird sich voraussichtlich auch 2024 fortsetzen. KI spielt nicht nur eine zentrale Rolle in der Cybersecurity, sondern ist auch in vielen anderen Bereichen fest etabliert. Ihre vielseitigen Einsatzmöglichkeiten erleichtern zahlreiche Arbeitsprozesse, bringen jedoch gleichzeitig neue Herausforderungen mit sich – insbesondere im Hinblick auf die Cybersecurity.

Die zunehmende Nutzung von KI durch Unternehmen hat dazu geführt, dass auch Cyberkriminelle diese Technologie vermehrt für ihre Zwecke einsetzen. KI-basierte Angriffe werden immer ausgefeilter, da die Technologie es ermöglicht, fortschrittliche Malware zu

entwickeln, Schwachstellen gezielt zu identifizieren und Angriffe effektiver zu gestalten. Begriffe wie Social Engineering, Phishing und Deepfakes stehen sinnbildlich für die neuen Bedrohungen, die durch KI verstärkt werden.

2024 wird daher eine entscheidende Herausforderung darin bestehen, KI-Technologien nicht nur effizient, sondern auch verantwortungsbewusst zu nutzen. Unternehmen müssen ihre KI-Systeme so absichern, dass ein Missbrauch durch Angreifende verhindert wird. Dies erfordert eine enge Zusammenarbeit zwischen IT- und Sicherheitsexperten, um sicherzustellen, dass die KI-Systeme stets auf dem neuesten Stand der Sicherheitsstandards sind.

Nur durch proaktives Handeln und eine bewusste Integration von Sicherheitsmaßnahmen können die Chancen von KI genutzt und gleichzeitig die Risiken minimiert werden.

Cyber-Security-Trend 2: Zunehmende Professionalisierung der Cyberkriminalität

Die Professionalisierung der Cyberkriminalität hat in den vergangenen Jahren stark zugenommen und wird auch im Jahr 2024 weiter an Bedeutung gewinnen. Cyberkriminalität hat sich zu einem lukrativen Wirtschaftsfaktor entwickelt, der es Angreifenden ermöglicht, erhebliche Gewinne zu erzielen. Gleichzeitig war es noch nie so einfach, in diese kriminelle Welt einzutauchen.

Besonders besorgniserregend ist der anhaltende Aufstieg des „Cybercrime as a Service (CaaS)"-Marktes, der 2024 ein weiteres Boom-Jahr erleben könnte. Dieses Modell bietet selbst technisch weniger versierten Personen die Möglichkeit, kriminelle Dienstleistungen anzubieten. In einem kürzlich veröffentlichten Blogbeitrag (Link) haben wir die Mechanismen und Auswirkungen von CaaS genauer beleuchtet. Dieser Trend verdeutlicht, wie stark die Professionalisierung vorangeschritten ist: Immer mehr Werkzeuge und Dienstleistungen stehen potenziellen Angreifenden zur Verfügung, was die Bedrohungslage weiter verschärft.

Für Unternehmen bedeutet dies, dass sie 2024 verstärkt in ihre Abwehrmechanismen investieren und sich auf eine neue Qualität von Bedrohungen einstellen müssen. Gleichzeitig wird die Zusammenarbeit zwischen Regierungen, Unternehmen und Sicherheitsdienstleistern von zentraler Bedeutung sein, um den wachsenden Herausforderungen durch die Professionalisierung der Cyberkriminalität effektiv entgegenzuwirken und eine sichere digitale Zukunft zu gewährleisten.

Cyber-Security-Trend 4: Bedrohungslage wächst weiter

Von Ransomware-Angriffen über politisch motivierte Cyberattacken bis hin zu Angriffen auf IoT-Infrastrukturen und Supply-Chain-Systeme: Die Bedrohungslage ist vielfältiger denn je und fordert von Unternehmen und Organisationen erhöhte Wachsamkeit sowie proaktive Gegenmassnahmen. Ein ganzheitlicher Sicherheitsansatz, der moderne Technologien einsetzt, Mitarbeitende gezielt schult und auf starke Partnerschaften innerhalb der Branche setzt, ist unverzichtbar. Angesichts der schnellen Weiterentwicklung von Cyber-Bedrohungen müssen

Sicherheitsstrategien zudem kontinuierlich angepasst werden, um einen wirksamen Schutz gegen die vielfältigen Gefahren sicherzustellen.

Quintessenz: Es gibt keine perfekte Lösung, um alle Cyberrisiken zu eliminieren, aber es gibt Maßnahmen, die das Risiko erheblich reduzieren:

1. **Bewusstsein schärfen**: Schulungen zu Cybersicherheit für Mitarbeiter und Privatpersonen sind der erste Schritt.
2. **Starke Passwörter und Multi-Faktor-Authentifizierung (MFA)**: Einfache Passwörter sind ein Einfallstor. MFA bietet eine zusätzliche Sicherheitsebene.
3. **Regelmäßige Updates**: Halten Sie Software und Betriebssysteme stets auf dem neuesten Stand, um bekannte Schwachstellen zu schließen.
4. **Antivirus- und Firewall-Lösungen**: Diese Werkzeuge sind essenziell, um Malware und andere Bedrohungen zu blockieren.
5. **Backups erstellen**: Regelmäßige Backups stellen sicher, dass wichtige Daten im Falle eines Angriffs wiederhergestellt werden können.

Cybersicherheit ist kein Luxus, sondern eine grundlegende Notwendigkeit. In einer vernetzten Welt, in der Daten einen unschätzbaren Wert haben, ist der Schutz dieser Daten von höchster Priorität. Indem wir uns der Risiken bewusst sind und geeignete Schutzmaßnahmen ergreifen, können wir dazu beitragen, die digitale Welt sicherer zu machen.