DIE TRENDS FÜR 2023:

IT-Sicherheit

Ob die Kompromittierung geschäftlicher E-Mails, Active-Directory-Angriffe, Ransomware, Phishing oder MFA-Attacken: Fundamentale Angriffe auf Organisationen bleiben auch 2023 sehr effektiv und lukrativ für Cyber-Kriminelle. Menschliche Fehler verursachen immer wieder Lücken in den bestehenden Cyber-Abwehrsystemen von Unternehmen. Zudem sind Phishing und neue MFA-Bombardements heute ausgefeilter denn je und verringern die Wirksamkeit von Sicherheitsschulungen.

Vor diesem Hintergrund sollten die Sicherheitsteams von Unternehmen nicht defensiv auf menschengemachte Probleme reagieren, sondern offensiv handeln. So ist zu hoffen, daß Kunden von MDR-Services (Managed Detection and Response) vor allem präventive Funktionen anstelle von reaktiven Schnellreparaturen fordern.

Zero Trust statt VPN

Viele Menschen arbeiten heute von zuhause – das ist nichts Neues. Neu ist dagegen die Art und Weise, wie die Sicherheitsteams die verteilt arbeitenden Beschäftigten schützen. Ab dem kommenden Jahr wird Zero Trust die virtuellen privaten Netzwerke (VPN) vollständig ersetzen. Die Grenzen der Unternehmensnetzwerke haben sich verschoben, da die Mitarbeiter auf einen Großteil ihrer Anwendungen via SaaS (Software-as-a-Service) zugreifen. Und die Absicherung von Heimnetzwerken ist für IT-Teams riskant. Um die vielerorts remote arbeitende Belegschaft unterstützen und schützen zu können, ist es daher entscheidend, grundsätzlich keinem Gerät zu vertrauen.

Erkaufter Zugang zu Unternehmensnetzen

Unserer Einschätzung nach wird Software-Hacking ab 2023 zurückgehen, dafür erhöht sich das „Insider-Risiko“. Das heißt, Hacker werden zunehmend Mitarbeiter von Drittanbietern für die Logistik sowie Internet Service Provider (ISP) und Softwarehersteller ins Visier nehmen und versuchen, sich den Zugang zum Firmennetzwerk zu erkaufen. Wichtig ist daher, daß Unternehmen nicht nur ihre eigenen Netzwerkgrenzen absichern, sondern auch darauf achten, daß ihre Zulieferer zuverlässig sind.

Weniger Passwörter

Die jüngste Sicherheitslücke bei Uber hat die Schwächen der Multifaktor-Authentifizierung (MFA) aufgezeigt. Es ist nicht davon auszugehen, daß die MFA-Müdigkeit dazu führt, daß Passwörter 2023 komplett verschwinden. In den kommenden Jahren wird ihre Verwendung jedoch abnehmen. Stattdessen werden sich andere Schutzmaßnahmen durchsetzen – darunter auch stärkere Kennwörter. Außerdem werden Passwort-Manager im nächsten Jahr allgegenwärtig sein, was sie wiederum zu einem wertvolleren Ziel für Hacker macht.

Strengere Sicherheitsmaßnahmen erwartet

Angesichts der wirtschaftlichen Lage ist es wahrscheinlich, daß Unternehmen aller Größen und Branchen Budget- und Personalkürzungen vornehmen werden. Wir glauben aber, daß die Sicherheitsteams davon weitgehend unberührt bleiben. Wegen der bevorstehenden wirtschaft-

Bild: philipp-katzenberger-iIJr-UoeRoCQ-unsplash

lichen Schwierigkeiten müssen sie allerdings künftig intelligenter arbeiten und sich konsolidieren. Als Zeichen für die große Bedeutung der Unternehmenssicherheit werden sich zudem Cyber-Security-Labels auf Produkten durchsetzen – speziell auf Hardware. Zudem dürften die US-amerikanischen Datenschutzgesetze auf das Niveau der europäischen Standards angehoben werden. Das bedeutet, daß Vorstände und Geschäftsleitung auf die Einhaltung strengerer Sicherheitsvorschriften achten müssen.

Mehr Kontrolle für Blockchains

Für Blockchain-Technologien war 2022 in Sachen Sicherheit ein schwieriges Jahr. 2023 könnte ähnlich turbulent werden, wenn der Code der Blockchain weiter als Gesetz gilt. Derzeit wird den Entwicklern und ihren Programmierkenntnissen zu viel Vertrauen geschenkt. Blockchain-Sicherheitsteams benötigen robustere Kontroll-, Erkennungs- und Reaktionsmöglichkeiten, um Angreifer abzuschrecken. Die zahlreichen Bridge-Hacks im Jahr 2022 haben das Vertrauen der Nutzer in die Blockchain-Security erschüttert. Glücklicherweise machen sich die Kunden genauso viele Gedanken über die Sicherheit der von ihnen gewählten Blockchain und über deren Funktionen. Daher werden sie für Blockchains im Jahr 2023 wahrscheinlich mehr Ressourcen zur Verbesserung der Sicherheit bereitstellen. Neben der Diebstahlbekämpfung sollten künftig vor allem die Verfügbarkeit und die Stabilität von Kryptowährungen Priorität haben. Denn wenn die Ausfälle und Verzögerungen anhalten, könnten einige Blockchains Nutzer verlieren und zusammenbrechen.

Sicherheitslektionen für die kommenden Jahre

Aus den Sicherheitsverletzungen, Hacks und Cyberpannen des Jahres 2022 können Securityexperten vor allem die folgenden Lehren für die Zukunft ziehen:

- MFA ist nicht vertrauenswürdig
- Alle Stakeholder – auch die Führungsriege – müssen Einblick in die Sicherheitslage ihres Unternehmens haben
- Es lohnt sich nicht, für eine einprozentige Verbesserung eines Produkts die IT-Sicherheit aufs Spiel zu setzen. Denn durch das ständige Umgestalten der IT-Architektur entstehen immer wieder neue Lücken
- Auch für die Blockchain ist kontinuierliche Sicherheit ein Muß. Statt einer einmaligen Bewertung bei der Markteinführung sollte das Securityteam auf eine kontinuierliche Validierung setzen.

Sicherheit beim Quantencomputing

Es ist eher unwahrscheinlich, daß es bereits 2023 zu einem massenhaften Einsatz von Quantencomputern kommen wird. Aber ab 2024 sollten die Sicherheitsexperten das Thema auf dem Schirm haben. Die derzeitigen Risiken beim Quantencomputing überwiegen nicht ganz die enormen Investitionen, die damit verbunden sind. Daher sollten Unternehmen, die auf die neue Technologie angewiesen sind, am besten schon jetzt mit der Risikobewertung beginnen. <<

Noch Fragen?
www.kudelskisecurity.com/de