WHITEPAPER

11 Sicherheitskontrollen zur Reduzierung von Cyberrisiken

Praktische Tipps für eine stärkere Cyberabwehr, mehr Resilienz und ein geringeres unternehmerisches Risiko

SOPHOS

Kurzfassung

Für jede Unternehmensführung ist es heute unerlässlich, zu verstehen, dass die Optimierung von Sicherheitskontrollen mehr bedeutet als nur den Schutz von Daten und Systemen. Im Fokus steht vielmehr die Minimierung unternehmerischer Risiken, um das Markenimage, das Vertrauen der Kunden und die Kontinuität des Geschäftsbetriebs nachhaltig zu sichern. Cyberangriffe wie Ransomware und Business Email Compromise (BEC) können erhebliche betriebliche und finanzielle Folgen haben. Laut Cyber Defense Magazine besagen Prognosen, dass Cyberkriminalität im Jahr 2025 weltweit 1,2 Billionen US-Dollar an Kosten verursachen wird[1]. Auch abgeschwächte Angriffe können den Betrieb schwer stören, wenn Systeme offline genommen werden müssen, um sie zurückzusetzen und neu aufzubauen. Manche Unternehmen stecken das locker weg. Für andere kann es jedoch schnell existenziell werden, wenn sie mit Herausforderungen konfrontiert sind, mit denen sie nie gerechnet hätten.

1,2 Billionen USD

Im Jahr 2025 wird Cyberkriminalität die Welt voraussichtlich 1,2 Billionen US-Dollar kosten.[1]

Die Rolle von Sicherheitskontrollen bei der Cyberabwehr-Optimierung

Sicherheitskontrollen sind die Hebel, die Sicherheitsteams nutzen können, um Risiken zu reduzieren und das Unternehmen vor Bedrohungen zu schützen. Es gibt viele Arten von Kontrollen, und sie alle haben das gleiche Ziel: Sicherheitsereignisse und -verletzungen zu verhindern bzw. den Schaden bei einem Vorfall zu minimieren. Manche dieser Kontrollen sind auf Prävention ausgerichtet, andere bieten verschiedene Stufen der Schadensbegrenzung in den Bereichen Abwehr, Erkennung und Reaktion auf Bedrohungen. Die richtige Mischung starker Sicherheitskontrollen in allen Bereichen ist wichtig, um eine umfassende Cyberabwehr aufzubauen.

Starke Sicherheitskontrollen sind auch ein wichtiger Bestandteil des Risikomanagements von Cyberversicherungen. Bei der Festlegung der Prämien und Deckungsgrenzen schauen Versicherungsunternehmen genau darauf, welche Kontrollen Unternehmen umsetzen.

Die Policen decken in der Regel Folgendes ab:

Eigenschadenhaftung für direkte Schäden, die Ihrem Unternehmen durch einen Cyberangriff oder eine Sicherheitsverletzung entstehen können. Dazu können Unterbrechungen des Geschäftsbetriebs, Kosten der Datenwiederherstellung, Datendiebstahl oder Ransomware-Zahlungen gehören.

Haftpflicht gegenüber Dritten bei Schäden durch Kunden, Partner, Aufsichtsbehörden oder andere. Hierzu gehören Rechtsstreitigkeiten, Schadenersatzforderungen oder Bußgelder von Regierungsbehörden und/oder Wirtschaftsverbänden.

Warum ist das wichtig?

Bessere Kontrollen schützen nicht nur Ihren Betrieb, sondern können Versicherungsprämien senken und im Schadensfall für bessere Ergebnisse sorgen.

Mit diesen 11 Sicherheits-kontrollen reduzieren Sie das Cyberrisiko

Die Investition in wirksame Kontrollen trägt zur Reduzierung von Cyberrisiken bei und kann die Versicherbarkeit sowie die Versicherungsbedingungen verbessern. In diesem Whitepaper führen wir elf grundlegende Kontrollmechanismen auf, mit denen Sie Ihre Cyberabwehr in verschiedenen Kategorien der Prävention und Schadensminderung stärken können.

Wenn Sie diese korrekt umsetzen, können Sie Ihren aktuellen Cybersicherheitsstatus bei aktuellen und künftigen Bedrohungen deutlich verbessern.

1. Identitäts- und Zugriffsverwaltung
2. Endpoint Security
3. Multi-Faktor-Authentifizierung (MFA)
4. Schwachstellen-Management
5. Email Security
6. Privileged Session Management
7. Asset Management
8. Segmentierung und Architektur
9. Extended Detection and Response (XDR)
10. Backup und Geschäftskontinuität
11. Netzwerksicherheit und Traffic-Überwachung

1. Identitäts- und Zugriffsverwaltung

Die Identitäts- und Zugriffsverwaltung stellt sicher, dass nur autorisierte Personen Zugriff auf Systeme und Daten erhalten. Mit dem Privileged Access Management (PAM) wird der Zugriff der Benutzer noch weiter eingegrenzt, und zwar nur auf das, was sie wirklich benötigen. Was einfach klingt, kann sich schnell komplex werden, insbesondere in größeren Unternehmen. Alle Unternehmen sollten strenge Onboarding-/Offboarding-Prozesse etablieren, starke Passwörter durchsetzen und den Zugriff regelmäßig überprüfen.

Unabhängig von der Größe muss jedes Unternehmen über klare Regeln für das Löschen alter Identitäten verfügen. Andernfalls können Angreifer diese vergessenen Konten ausnutzen, um ihre Berechtigungen zu erweitern und sich unbemerkt in Ihrer Umgebung zu bewegen.

2. Endpoint Security

Jedes Gerät, das mit Ihrer Umgebung verbunden ist, stellt ein potenzielles Risiko dar. Durch das Aufkommen neuer hybrider Arbeitsmodelle hat sich diese Anfälligkeit noch erhöht, weshalb Endpoint Protection heute wichtiger ist denn je. Viele Angriffe beginnen mit „Standard"-Bedrohungen, die mit wenig Aufwand verbunden sind. Diese werden von leistungsstarken Endpoint-Tools zuverlässig erkannt und neutralisiert. Endpoints, die nicht mehr unterstützt werden oder gar nicht mehr bekannt sind, können sich jedoch zu Schwachstellen und zu einem Einstiegspunkt für Remote-Ransomware-Angriffe entwickeln. Stellen Sie sicher, dass jedes Gerät vom Ihrem Schutz abgedeckt ist.

3. Multi-Faktor-Authentifizierung (MFA)

Multi-Faktor-Authentifizierung (MFA) überprüft die Identität der Benutzer anhand mehrerer Faktoren: etwas, das sie wissen (z. B. Passwort), etwas, das die besitzen (z. B. ein Token), etwas, das zu ihrer Person gehört (z. B. Fingerabdruck). Da kompromittierte Zugangsdaten nach wie vor eine der Hauptursachen für Angriffe sind,[2] stellt MFA eine wichtige Kontrollmaßnahme für moderne Unternehmen dar. Erwägen Sie fortschrittlichere Methoden wie die Geolokalisierung oder den numerischen Abgleich, um sich gegen die Umgehungstaktiken von Angreifern besser zu schützen und gleichzeitig ein Gleichgewicht zwischen der Benutzererfahrung und dem Datenschutz herzustellen.

Tipps

Inaktive Konten und ungenutzte Berechtigungen sind leicht zugängliche Angriffspunkte. Sobald sich die Angreifer im Inneren Ihres Systems befinden, können sie dazu genutzt werden, sich einen erweiterten Zugriff zu verschaffen und die Reichweite des Angriffs unbemerkt zu vergrößern.

Der häufigste Einstiegspunkt ist oft der am wenigsten sichtbare. Lassen Sie nicht zu, dass veraltete Endpoints zu Sicherheitslücken werden.

Setzen Sie auf adaptive MFA, um die Verifizierung in Hochrisikoszenarien zu verbessern, ohne dabei unnötige Reibungen zu verursachen.

4. Schwachstellen-Management

Das Schwachstellen-Management meint den fortlaufenden Prozess der Identifizierung, Bewertung und Behebung von Sicherheitslücken in Ihrer gesamten Umgebung. Hierzu gehören gängige Praktiken wie Software- und System-Patching, Konfigurationsaktualisierungen und die Überwachung neu bekannt gewordener Sicherheitslücken. Eine zuverlässige Bedrohungsanalyse ist von entscheidender Bedeutung, um aufkommende Risiken frühzeitig zu erkennen.

Es ist für Ihr Unternehmen unerlässlich, zu wissen, wo in Ihrem Netzwerk sich die Geräte befinden, damit der Scan umfassend erfolgen kann. Dank dieser umfassenden Transparenz können Unternehmen einen risikobasierten Ansatz verfolgen, um zu priorisieren, welche Schwachstellen zuerst behoben werden müssen – basierend auf der Exposition, der Wahrscheinlichkeit eines Angriffs und den Auswirkungen auf das Geschäft.

5. Email Security

Obwohl es sich um eine ältere Technologie handelt, ist und bleibt die E-Mail einer der häufigsten Angriffspunkte. Insbesondere das Phishing wird nach wie vor von Ransomware und für den Diebstahl von Zugangsdaten genutzt. Business Email Compromise (BEC) gehört zu den häufigsten Cyberversicherungsfällen.[3] Mit einer starken E-Mail-Sicherheit können Sie verhindern, dass bösartige Inhalte in die Posteingänge Ihrer Benutzer gelangen, was sie zur wichtigen ersten Verteidigungslinie macht. Durch generative KI werden die Phishing-Taktiken mit verbesserter Grammatik und Nachrichtenübermittlung immer weiter optimiert. Deshalb ist es unerlässlich, auch die Schutzmaßnahmen zu erweitern, um die Erfolgsquote dieser Angriffe zu verringern, bevor sie die Benutzer erreichen.

Der Schutz sollte jedoch nicht bei der Zustellung enden. URLs und Anhänge, die auf den ersten Blick sicher wirken, können bösartig werden, wenn sie sich im Posteingang befinden. Fortschrittliche E-Mail Security-Lösungen bieten aus diesem Grund eine Erkennung und Behebung von Angriffen nach der Zustellung an – sie scannen Inhalte automatisch erneut, ziehen bösartige Nachrichten zurück und neutralisieren Links, wenn sich deren Risikoprofil ändert. Diese Kontrollen können helfen, Bedrohungen zu erkennen, die die ersten Abwehrmaßnahmen umgehen, und die Verweildauer schädlicher Nachrichten in den Benutzer-Posteingängen auf ein Minimum zu reduzieren.

Tipps

Suchen Sie nach Schwachstellen in Ihren Anwendungen von Drittanbietern und Cloud-Diensten – nicht nur in Ihren Kernsystemen.

Ein Klick genügt. Der beste Weg, Phishing zu verhindern, ist sicherzustellen, dass die Benutzer den Köder niemals zu Gesicht bekommen – auch nicht nach der Zustellung.

6. Privileged Session Management

Administrative Konten bieten Angreifern die größte Macht – insbesondere, wenn sie Berechtigungen für den Zugriff auf Identitätssysteme, Konfigurationskontrollen und Sicherheitstools umfassen. Wenn ein Angreifer Administratorrechte erlangt, kann er Schutzmaßnahmen deaktivieren und Ransomware im großen Maßstab einbringen.

Dieses Risiko kann verringert werden, indem Unternehmen ein mehrstufiges Modell für die Zugriffsberechtigung implementieren und aktiv überwachen, wie diese Konten genutzt werden. Das Privileged Session Management (PSM) bietet Überwachung mittels Protokollierung, Aufzeichnung und in manchen Fällen auch mittels Steuerung der Administratorsitzungen in Echtzeit. Das hilft, verdächtige Aktivitäten zu erkennen, Missbrauch zu verhindern und die Einhaltung von Vorschriften zu fördern.

7. Asset Management

Sie können nur das schützen, von dem Sie wissen, dass Sie es besitzen. Darum müssen Unternehmen stets aktuelle Bestandslisten sowohl ihrer physischen Geräte als auch ihrer Daten führen. Während eines Vorfalls ist es für eine schnelle und effektive Untersuchung, eine genaue Berichterstattung und eine schnelle Eindämmung unerlässlich, genau zu wissen, wo die sensiblen Daten gespeichert sind. Ein korrektes Asset Management ist die Basis für eine gründliche Untersuchung, trägt zur Optimierung der Zuständigkeiten bei und verringert die Auswirkungen einer Datenschutzverletzung.

8. Segmentierung und Architektur

Nachdem ein Angreifer Zugriff auf Ihre Umgebung erhalten hat, bewegt er sich in dieser anschließend meist lateral – mit dem Ziel, seine Berechtigungen zu erweitern, auf sensible Systeme zuzugreifen oder Ransomware einzusetzen. Dies kann durch eine starke Netzwerksegmentierung und ein entsprechendes Architekturdesign erheblich erschwert werden. Segmentierung erzeugt Reibung und macht Angreifer sichtbarer, was Ihre Chancen erhöht, Angriffe früher zu erkennen.

Darum sollte Ihre Systemarchitektur auf den Prinzipien der Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit basieren. Dazu gehören die Zugriffsbeschränkung von System auf System und von Benutzer auf System mittels eines Zero-Trust-Modells, bei dem jede Transaktion auf Basis der Identität, des Geräts und der Berechtigungen des Benutzers überprüft wird.

Tipps

Können Sie nachvollziehen, wer am vergangenen Dienstag auf Ihre Administrationsebene zugegriffen und welche Aktionen durchgeführt hat? Wenn nicht, ist es an der Zeit, die Transparenz zu erhöhen.

An nicht benötigten Aufzeichnungen festzuhalten kann die Versicherungskosten erhöhen und den Reputationsschaden im Falle einer Datenschutzverletzung vervielfachen.

Nutzen Sie Netzwerksegmentierung, um kritische Systeme von Access Points zu isolieren.

9. Extended Detection and Response (XDR)

Wenn viele unterschiedliche Tools zum Einsatz kommen, kann dies Warnmeldungen fragmentieren, die Triage verlangsamen und Bedrohungsaktivitäten verschleiern. Mit Extended Detection and Response (XDR) wird dieses Problem behoben, indem es einen einheitlichen Überblick über die Aktivitäten der Endpoint-, Firewall-, Netzwerk-, E-Mail-, Identitäts-, Backup- und Cloud-Sicherheitssysteme hinweg sicherstellt. Das reduziert die Alarmhäufigkeit und ermöglicht eine schnellere, sicherere Entscheidungsfindung. Der sogenannte „Drehstuhl"-Effekt, also das Hin- und Herspringen zwischen isolierten Analyse-Tools, entfällt bei der Untersuchung und Reaktion auf Bedrohungen.

Robuste XDR-Systeme nutzen darüber hinaus fortschrittliche Analysen, KI-basierte Priorisierung der Erkennung, tiefgehende Datensuche sowie automatisierte Korrelation und Eskalation von Warnmeldungen. Mit diesen Funktionen zusammengenommen werden die Erkennungsgenauigkeit verbessert, Untersuchungen beschleunigt und Sicherheitsteams unterstützt, sich auf die riskantesten Bedrohungen zu konzentrieren, ohne sich dabei mit Problemen bei der Nutzung der Tools auseinandersetzen zu müssen.

10. Backup und Geschäftskontinuität

Wenn ein Cybervorfall den Betrieb stört oder Systeme beschädigt, können gut vorbereitete Backups und ein solider Plan für Geschäftskontinuität den entscheidenden Unterschied zwischen einer schnellen Wiederherstellung und längeren Ausfallzeiten ausmachen. Jedoch ist Backup nicht gleich Backup. Um effektiv zu sein, müssen Backups validiert, regelmäßig getestet und in der Lage sein, Systeme und Daten mit Integrität wiederherzustellen.

Häufig passieren Fehler schon bei der Einrichtung. Viele Unternehmen stellen erst viel zu spät fest, dass sie mit den Backups ihre Systeme nur teilweise wiederherstellen können oder dass wichtige Daten fehlen. Ein kurzfristiger Ausfall kann sich daher zu einer wochenlangen Herausforderung entwickeln.

Ebenso ist es wichtig, dass Backups durch eine Out-of-Band-Authentifizierung geschützt werden. Ohne diese können Angreifer im Rahmen eines Angriffs mit erweiterten Zugriffsrechten versuchen, die Backup-Daten zu deaktivieren oder zu löschen.

Tipps

XDR verwandelt isolierte Warnmeldungen in entschiedenes Handeln, beschleunigt Untersuchungen und verbessert die Ergebnisse von Reaktionen.

Bewahren Sie Backups nach Möglichkeit segmentiert und offline auf. Ihre Backup- und Wiederherstellungslösung sollte niemals von nur einem einzigen Kanal abhängig sein.

11. Netzwerksicherheit und Traffic-Überwachung

Das Netzwerk ist mehr als nur eine Verbindungsschicht – es ist ein strategischer Kontrollpunkt für die Überprüfung, Filterung und Verwaltung des Traffics in Ihrer gesamten Umgebung. Firewalls, Intrusion Prevention-Systeme (IPS), DNS-Filterung und sichere Web-Gateways bilden das Rückgrat eines mehrschichtigen Schutzes.

Allerdings sind nicht alle Firewalls gleichwertig. Veraltete, falsch konfigurierte oder unzureichend genutzte Lösungen können Sicherheitslücken aufweisen. Die regelmäßige Überprüfung, Aktualisierung und Anpassung Ihres Verteidigungssystems an die aktuelle Bedrohungslandschaft sind für die Aufrechterhaltung Ihrer Resilienz von entscheidender Bedeutung.

Mit modernen Kontrollmechanismen wie Zero Trust Network Access (ZTNA) kann eine granulare, kontextbezogene Durchsetzung von Zugriffsrechten sichergestellt werden. In Verbindung mit den herkömmlichen Schutzmaßnahmen tragen sie so dazu bei, die Angriffsfläche zu verringern, laterale Bewegungen zu verhindern und die Exfiltration in Hybrid- und Cloud-Umgebungen zu unterbinden.

Tipps

Integrieren Sie Netzwerktelemetrie in Ihren Erkennungs-Stack, um die Transparenz zu verbessern, Untersuchungen zu beschleunigen und anomale Aktivitäten zu kennzeichnen – insbesondere laterale Bewegungen und Command-and-Control-Datenverkehr.

Vom ganzheitlichen Überblick zum ganzheitlichen Ansatz

Bei Cybersicherheit geht es nicht nur darum, die richtigen Tools einzusetzen, sondern auch darum, eine Strategie zu entwickeln, die Menschen, Prozesse und Technologie miteinander verknüpft. Mit diesen 11 Kontrollen können Sie das Risiko für Ihr Unternehmen bei sorgfältiger und konsequenter Umsetzung erheblich reduzieren.

Langfristige Resilienz entsteht durch den Aufbau eines robusten Cybersicherheitssystems, das wiederholt funktioniert, anpassungsfähig ist und auf klaren Zuständigkeiten basiert. Technik ist per se leistungsstark, jedoch kann nur durch qualifizierte Teams und strukturierte Prozesse sichergestellt werden, dass sie auch wirksam eingesetzt wird.

Bedrohungen entwickeln sich stets weiter, Technologien werden sich verändern und Ihr Unternehmen wird sich wandeln. Um mithalten zu können, ist es unerlässlich, ganzheitlich zu denken, sich kontinuierlich anzupassen und eine Kultur zu etablieren, in der Sicherheit nicht nur lästige Notwendigkeit ist, sondern ein zentraler Faktor für den Geschäftserfolg.

[1] Cyber Defense Magazine: The True Cost of Cybercrime: Why Global Damages Could Reach $1.2-$1.5 Trillion by End of Year 2025
2 Sophos, Annual Threat Report 2025
3 Dark Reading, „Email-Based Attacks Top Cyber-Insurance Claims“, 8. Mai 2025

Bereit, Ihr Cybersicherheits-programm zu bewerten?

Sprechen Sie noch heute mit einem Sophos-Experten.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel: +49 611 5858 0
E-Mail: sales@sophos.de