FORTINET

Weniger Komplexität bei der Security durch Integration und Automatisierung

4 Strategien für CIOs

Inhaltsverzeichnis

FORTINET

Zusammenfassung

CIOs beschleunigen Geschäftszyklen und ermöglichen vollkommen neue Funktionen durch innovative Tools – wie cloudbasierte Anwendungen oder intelligente DevOps-Prozesse bei der Software-Entwicklung. Doch diese digitalen Innovationen bringen nicht nur mehr Produktivität, sondern auch neue Risiken mit sich. Wenn CIOs die Geschwindigkeit und Komplexität von Netzwerk-Infrastrukturen erhöhen, müssen sie auch eine geeignete Cyber-Security implementieren, damit Systeme, Daten und Anwender bei schnellen Änderungen sicher geschützt sind. Fortinet unterstützt CIOs dabei, die Netzwerk-Security zu vereinfachen und zugleich die Kosten zu senken, die mit dem ständigen Hinzufügen isolierter Produkte bei neuen Bedrohungen einhergehen.

01 Einleitung: Komplexität ist der Feind der Sicherheit

Zweifellos begrüßen CIOs strategische Innovationen, da sie geschäftliche Effizienz und Effektivität versprechen. Schließlich ermöglichen transformative digitale Technologien neue Funktionen und Wachstum in allen Branchen. Auch tragen Neuerungen – wie cloudbasierte Anwendungen, IoT-Geräte (Internet der Dinge) sowie interne oder externe DevOps-Services in der Entwicklung – durch Automatisierung zu Produktivitätssteigerungen, besserer Skalierbarkeit, Kostensenkungen und kürzeren Markteinführungszeiten bei.

Die Auswirkungen dieser Änderungen auf Unternehmen sind jedoch nicht durchweg positiv. Netzwerke werden immer komplexer, wodurch eine erweiterte Angriffsfläche mit neuen Risiken entsteht. Oft werden dann als Reaktion auf Bedrohungen isolierte Einzellösungen implementiert. Doch aus sicherheitsstrategischer Sicht ist dies nicht mehr als ein ineffizientes, kostspieliges „Stückwerk“, das weder Security- noch Compliance-Anforderungen erfüllen kann. Laut einer kürzlich durchgeführten Befragung von CIOs verlassen sich 77 % der Unternehmen in gewissem Maß auf nichtintegrierte Einzelprodukte, wodurch Lücken bei der Sicherheitseffektivität entstehen.[1]

Erschwerend kommt hinzu, dass immer strengere Compliance-Vorschriften – wie die Datenschutz-Grundverordnung der Europäischen Union (DSGVO) oder die Sicherheitsstandards des National Institute of Standards and Technology (NIST) – verlangt werden. Unternehmen müssen die von ihnen erzeugten Datenmassen verwalten, kontrollieren und deren Regelkonformität sicherstellen. Dies wird immer schwieriger, wenn auch private Geräte von Mitarbeitern, nicht gepatchte Software infolge einer „Schatten-IT“ und das Management von Lieferanten und Partnern mit Netzwerk-Zugriff berücksichtigt werden müssen.[2]

Diese ineinandergreifenden Entwicklungen führen dazu, dass von CIOs mehr Technologiekompetenz und Führungsqualitäten erwartet werden.[3] CIOs können mit diesen Anforderungen Schritt halten, wenn sie die Problematik einer komplexen Security angehen und sich auf vier strategische Lösungsbereiche konzentrieren:

- **integrierte Sicherheit**
- **automatisierte Security-Workflows**
- **automatisierte Compliance-Governance**
- **einfacheres Risiko-Management**

78 %

der CIOs sind der Meinung, dass ihre digitale Strategie nur mäßig effektiv ist – oder noch schlechter greift.[4]

02 Integrierte Sicherheit

Neben der Erweiterung der Angriffsfläche nehmen auch die Anzahl und die Komplexität von Bedrohungen zu, die auf Netzwerk-Schwachstellen abzielen. Durch die weitverbreitete Ergänzung vorhandener Sicherheitslösungen durch Einzelprodukte, um neue Sicherheitslücken zu schließen, ist in den meisten Unternehmen eine unzusammenhängende Sicherheitsinfrastruktur entstanden.

Dieser Mangel an Integration schafft zwei große Probleme für CIOs: Erstens sind nur begrenzte Informationen über Bedrohungen verfügbar. Security-Einzellösungen können keine Informationen über potenzielle Bedrohungen im gesamten Unternehmen austauschen. Entsprechend langsam und ineffizient erfolgen koordinierte Reaktionen, wenn das Unternehmen an mehreren Stellen angegriffen wird. Zweitens zwingt die mangelnde Integration Unternehmen dazu, sich zu stark auf manuelle Prozesse zu verlassen – die von bereits überlasteten Security-Teams überwacht werden müssen. Die Zusammenstellung von Bedrohungsdaten und Audit-Trails für Compliance-Berichte durch Mitarbeiter ist zeitaufwendig, teuer, fehleranfällig und insgesamt ineffizient verglichen mit den ergänzenden automatisierten Funktionen, die eine integrierte Sicherheitsarchitektur bietet.

Eine integrierte Sicherheitsarchitektur verbindet unterschiedliche Sicherheitsprodukte zu einem zusammenhängenden System, das Echtzeitinformationen in allen Teilen des Unternehmens gemeinsam nutzt. Dieses unterstützt wiederum:

- vorkonfigurierte APIs (Application Programming Interfaces) sowie die Möglichkeit, diese APIs außerhalb der Architektur mit REST-APIs (Representational State Transfer) schnell zu integrieren,
- ein zentralisiertes Management (über eine zentrale Konsole) für transparente Sichtbarkeit und die Anwendung einheitlicher Richtlinien für alle implementierten Sicherheitslösungen im gesamten Unternehmen,
- ein offenes Ecosystem, in das Lösungen von Drittanbietern integriert werden können, um vorhandene Sicherheitsinvestitionen zu maximieren,
- die Reduzierung von Komplexität und Kosten, die ansonsten durch zusätzliche isolierte Produkte zur Abdeckung neuer Risiken entstehen,
- und was wahrscheinlich am wichtigsten ist: Es wird eine Grundlage für automatisierte Sicherheitsfunktionen geschaffen.

Das Fehlen einer durchgängigen Integration ist heute für fast ein Drittel (32 %) der CIOs eines der Hauptprobleme bei der Security.[5]

03 Automatisierte Security-Workflows

Bei einer weltweiten Befragung von CIOs gaben 65 % der Befragten an, dass der Fachkräftemangel sich negativ auf die Unternehmensentwicklung auswirkt.[6] Eine Automatisierung kann zur Lösung dieses Problems beitragen, da Security-Teams dadurch entlastet und fehlende Qualifikationen ergänzt werden. Mitarbeiter können sich dann auf anspruchsvollere Aufgaben wie die Risiko-Governance oder das Risiko-Management konzentrieren.

Manuelle Abläufe wie Implementierung, Bereitstellung, Untersuchung von Bedrohungsalarmen oder Zugangskontrollen für Benutzer und Geräte lassen sich komplett durch richtlinienbasierte Kontrollen automatisieren und orchestrieren. CIOs können somit Automatisierungsanforderungen in zwei Hauptbereichen des Incident-Response-Workflows erfüllen:

Network Operations Center (NOC) – Beispiele für sinnvolle Automatisierungen:

- DevOps-Sicherheitskontrollen, die das Time-to-Market verkürzen (statt es zu behindern)
- Zero-Touch-Bereitstellung in dezentralen Unternehmen
- Zugangsmanagement für Geräte und Anwender
- Echtzeit-Informationen über die Leistung des Filialnetzwerks, um Probleme wie Spikes, Skalierung und Prioritäts-Routing des Datenverkehrs leichter in den Griff zu bekommen

Security Operations Center (SOC) – Beispiele für sinnvolle Automatisierungen:

- proaktive Bedrohungserkennung
- Bedrohungskorrelationen und Austausch von Bedrohungsinformationen
- Warnmeldungen und Bedrohungsforschung/-analyse
- Reaktion auf Sicherheitsvorfälle und Einleitung von Gegenmaßnahmen

67 %

der CIOs planen den Einsatz von Automatisierungen, um keine weiteren Mitarbeiter einstellen zu müssen.[7]

04 Automatisierte Compliance-Governance

CIOs sollten nach Wegen suchen, um die Compliance-Governance zu automatisieren. Die kumulative Belastung durch eine manuelle Nachverfolgung und Berichterstellung zur Einhaltung von Industriestandards und Datenschutzgesetzen ist für das Unternehmen sowohl zeitaufwendig als auch kostspielig.

Angesichts der ersten hohen Bußgelder für Verstöße gegen die DSGVO[8] sollte die Compliance für Führungskräfte und Vorstandsmitglieder ein zentrales Anliegen sein. Die meisten Unternehmen müssen mit Audit-Trails die Einhaltung von Datenschutzgesetzen nachweisen – wie z. B. der bereits erwähnten DSGVO in der Europäischen Union oder des neuen kalifornischen Verbraucherschutzgesetzes (CCPA), des Health Insurance Portability and Accountability Act (HIPAA) und des Sarbanes-Oxley Act (SOX) in den USA. Auch die Regelkonformität mit etablierten Branchenvorschriften wie dem Zahlungsstandard PCI DSS (Payment Card Industry Data Security Standard) muss gegeben sein.

Die Einhaltung des Datenschutzes über den gesamten Lebenszyklus hinweg bringt zudem geschäftliche Vorteile, da Unternehmen so belegen können, dass sie das Vertrauen der Kunden verdienen.[9] CIOs wiederum sind direkt oder indirekt dafür verantwortlich, den Datenschutz für Kundendaten zu gewährleisten.[10] Mit zunehmenden Transparenzproblemen – beispielsweise in Folge einer „Schatten-IT“ – gestaltet sich diese Gewährleistung und Aufrechterhaltung der Compliance für CIOs immer komplexer. Denn es ist der CIO, der sicherstellen muss, dass vertrauliche Informationen nicht unkontrolliert in Systemen von Drittanbietern gespeichert werden.[11]

Sicherheitslösungen sollten daher sowohl Transparenz als auch Flexibilität für die Skalierung in einem wachsenden, sich schnell verändernden Netzwerk bieten. Auch muss dieses Verteidigungssystem flexibel genug sein, um wechselnden Sicherheits- und Compliance-Anforderungen gerecht zu werden – ohne dass jedes Mal die Sicherheitsinfrastruktur überarbeitet werden muss. Dazu gehört ein Reporting, das alle Elemente einer Security-Lösung umfasst und IT-Teams von zeitaufwendigen manuellen Log-Abfragen befreit. Automatische Funktionen für die Nachverfolgung der Regelkonformität und Compliance-Berichte sollten zudem benutzerdefinierte Dashboards für bestimmte Führungsrollen und Vorstandsmitglieder bereitstellen, um interne Kontrollen zu erleichtern.

69 %

der Unternehmen sehen in der Compliance einen steigenden Kostenfaktor.[12]

05 Einfacheres Risiko-Management

Beim Management und der Bewertung von Risiken müssen CIOs zudem bestimmte Sicherheitsstandards einhalten. Dazu gehören Standards und Normen wie **NIST**, **ISO** und **CIS (Center for Internet Security)**. Viele davon werden zu staatlichen De-facto-Standards: Beispielsweise befolgt schätzungsweise die Hälfte aller US-Unternehmen das NIST-Regelwerk bis 2020 zur Bewertung, Verfolgung und Meldung des Sicherheitsstatus, das auch im Gesundheitswesen, Einzelhandel, Finanzbereich und in allen Sektoren mit kritischer nationaler Infrastruktur als Leitlinie dient.[13]

Tools und Services für die **analysebasierte Risikobewertung** bieten dynamische Schwachstellen-Analysen und Vergleiche mit Marktbegleitern, damit CIOs den aktuellen Gefährdungsstatus des gesamten Unternehmens realistisch einschätzen können. Die Risikobewertung liefert messbare Benchmarks und hilfreiche Konfigurationsempfehlungen, um Risikoindikatoren zu definieren und das Sicherheitsprofil des Unternehmens zu verbessern. Eine Bewertung anhand mehrerer Faktoren kann potenzielle Schwachstellen beheben. Hierbei werden Zugriffshäufigkeit, Benutzeraktivität, Verbreitung und Volumen gezielt untersucht, um eine risikobasierte Priorisierung von Datenschutzproblemen zu ermöglichen.[14]

Eine **absichtsbasierte Segmentierung** hilft dabei, die Geschäftsabsicht effizient nach bestimmten Kriterien (Wo? Wie? Was?) zu „übersetzen“, um den Zugang zu sensiblen Daten und Systemen zu kontrollieren. Unternehmen erhalten damit eine feinmaschige Zugriffskontrolle, die anhand einer kontinuierlichen Bewertung der Anwender-Vertrauenswürdigkeit angepasst wird. Als Teil einer integrierten Sicherheitsarchitektur kann die absichtsbasierte Segmentierung das Verteidigungsprofil eines Unternehmens effektiv verbessern, Risiken eindämmen, die Compliance fördern und die betriebliche Effizienz steigern.

In einer aktuellen Umfrage nannten CIOs das Risiko-Management im Bereich Cyber-Security als wichtigstes Erfolgskriterium.[15]

06 Weniger Komplexität bei der Sicherheit: Checkliste für die Umsetzung

Innerhalb der vier oben genannten allgemeinen Lösungsbereiche sollten CIOs bei der Weiterentwicklung der Sicherheitsarchitektur auf folgende sechs Funktionalitäten achten, um eine größere Einfachheit und Effizienz zu erzielen:

- ☐ Integration, um unterschiedliche Sicherheitsprodukte zu einer kohärenten, intelligenten Sicherheitsarchitektur zu verbinden
- ☐ Management über eine zentrale Konsole, um Transparenz und Kontrolle über die gesamte Sicherheitsinfrastruktur zu erhalten
- ☐ Funktionen bzw. Lösungen zur Automatisierung von Workflows, um Implementierungen, Bedrohungsanalysen und das Zugangsmanagement zu vereinfachen und Kontextinformationen zu verbessern
- ☐ automatisiertes Tracking und Reporting für Compliance-Zwecke
- ☐ analysebasierte Risikobewertung zur Messung und Bedrohungsabwehr in Echtzeit
- ☐ absichtsbasierte Segmentierung zur granularen, richtlinienbasierten Kontrolle des internen Netzwerk-Traffics

[1] „State of the CIO and Security Report“. Fortinet, März 2019.

[2] Jennifer Lonoff Schiff: „5 biggest IT compliance headaches and how to address them“. CIO, 9. Mai 2018.

[3] „Role Of CIO Is Changing And Growing In Importance, Say New Forbes Insights Studies“. Forbes, 28. März 2018.

[4] „CIO Survey 2018: The Transformational CIO“. Harvey Nash und KPMG, 25. Mai 2018.

[5] „State of the CIO and Security Report“. Fortinet, März 2019.

[6] „CIO Survey 2018: The Transformational CIO“. Harvey Nash und KPMG, 25. Mai 2018.

[7] „CIO Survey 2018: The Transformational CIO“. Harvey Nash und KPMG, 25. Mai 2018.

[8] Adam Satariano: „Google Is Fined $57 Million Under Europe’s Data Privacy Law“. The New York Times, 21. Januar 2019.

[9] Nancy Couture: „How data governance can support data privacy compliance“. CIO, 7. Februar 2019.

[10] „State of the CIO and Security Report“. Fortinet, März 2019.

[11] „CIO Survey 2018: The Transformational CIO“. Harvey Nash und KPMG, 25. Mai 2018.

[12] Josh Fruhlinger: „Top cybersecurity facts, figures and statistics for 2018“.CSO, 10. Oktober 2018.

[13] Jonathan Nguyen-Duy: „The Cybersecurity Regulations Healthcare, Financial Services, and Retail Industries Must Know About“. Fortinet, 21. August 2018.

[14] Nancy Couture: „How data governance can support data privacy compliance“. CIO, 7. Februar 2019.

[15] „State of the CIO and Security Report“. Fortinet, März 2019.

www.fortinet.com/de

323378-0-A-DE

3. Dezember, 2019

ebook-untangling-security-complexity_DE