Leitfaden für Führungskräfte

BAHNBRECHENDER ERFOLG MIT MODERNER SICHERHEIT:

Wie CIOs die Ausfallsicherheit bei Cyberangriffen verbessern können

Cybersicherheit gehört derzeit zu den wichtigsten Prioritäten für CIOs.

Die jüngste rasante Beschleunigung der digitalen Transformation und die zunehmende Verbreitung des mobilen Arbeitsplatzes stellen ganz neue Anforderungen an die Cybersicherheit.

Als die meisten Beschäftigten ausschließlich im Büro arbeiteten, waren die Grenzen für Cybersicherheit klarer. Mit der mobilen Arbeit erweitert sich die Bedrohungsfläche auf alle Arbeitsorte Ihrer MitarbeiterInnen.

In der Breakthrough-Studie von Dell Technologies (basierend auf Untersuchungen mit mehr als 10.500 Beschäftigten an mehr als 40 Standorten) gaben

72 % der Befragten an, dass die sich verändernde Arbeitswelt ihr Unternehmen einem größeren Cybersicherheitsrisiko ausgesetzt hat.

Die Herausforderungen, mit der CIOs konfrontiert sind, entstehen an der Schnittstelle zwischen effektiven Cybersicherheitsmaßnahmen und der Praxis. Knapp zwei Drittel der Befragten (62 %) sind der Meinung, dass MitarbeiterInnen das schwächste Glied in ihrer Sicherheitslandschaft sind. Und die Beschäftigten bestätigen diese Besorgnis. Mehr als die Hälfte (56 %) geben an, dass sie ihr Sicherheitsbewusstsein oder ihr Verhalten nicht wesentlich geändert haben, selbst wenn sie sich der Risiken stärker bewusst sind.

Dies ist ein universelles und menschliches Problem – selbst die sicherheitsbewussteste Person kann Fehler machen. Die effektivste Strategie besteht nicht darin, die MitarbeiterInnen zur Einhaltung bestehender und möglicherweise veralteter Protokolle zu zwingen, sondern dafür zu sorgen, dass Ihre Sicherheitsvorkehrungen auch den menschlichen Faktor berücksichtigen.

Als CIO sind Sie für die Sicherung scheinbar unendlich vieler unsicherer Standorte verantwortlich. MitarbeiterInnen können zwar eine gewisse Mithilfe leisten, aber es reicht nicht aus, sich allein auf ihre Beteiligung zu verlassen. Diese Aufgabe mag gewaltig erscheinen, ist aber machbar.

Hier erfahren Sie mehr über die wichtigsten Sicherheitsvorkehrungen für Ihre MitarbeiterInnen und Ihre IT-Infrastruktur.

Dies sind die fünf wichtigsten Gründe, die nach Meinung der Befragten dazu führen, dass ihre MitarbeiterInnen Opfer von Cyberangriffen werden:

1. Übermäßiges Vertrauen in die Bedrohungsabwehr durch die Firewalls des Unternehmens
2. Fehlendes Bewusstsein für das Ausmaß der Bedrohung
3. Hoffnung, dass sie nicht zur Zielscheibe werden
4. Annahme, dass die Folgen leicht behoben werden können
5. Ignorieren der Bedrohung, weil sie nicht wissen, wie sie behoben werden kann

„Sicherheit liegt in der Verantwortung aller. Angesichts zunehmender Sicherheitsbedrohungen müssen Unternehmen ihren MitarbeiterInnen das richtige Wissen vermitteln. Sie müssen verstehen, dass sie dazu beitragen können, Cyberkriminelle abzuwehren, indem sie die Sicherheitsanforderungen ihres Unternehmens erfüllen. Unternehmen müssen dieses Verhalten auch durch die Bereitstellung von intrinsisch sicheren Technologien und Technologieprozessen zum Standard machen. Es ist von größter Bedeutung, die Botschaft der geteilten Sicherheitsverantwortung in der Unternehmenskultur zu verankern. Im Allgemeinen müssen Menschen eine Nachricht mehrmals und auf unterschiedliche Weise hören, bevor sie ihr Verhalten ändern."

John Scimone, Senior Vice President und Chief Security Officer, Dell Technologies

Sicherheitsvorkehrungen als Antwort auf unvorsichtiges Verhalten

CIOs und CISOs sind für die Bereitstellung von Technologie zur Sicherung der digitalen Ressourcen des Unternehmens verantwortlich. Aber was geschieht, wenn die unsichersten (und unbeständigsten) Elemente des Systems die Menschen sind, die es benutzen?

Selbst in bester Absicht sind menschliche Fehler unvermeidlich. Daher ist es nur eine Frage der Zeit, bis der Ernstfall eintritt. Aus diesem Grund ist es wichtig, einen Plan für den Moment zu haben, in dem Ihre Cybersicherheitsmaßnahmen dem ultimativen Test eines realen Cybersicherheitsangriffs unterzogen werden. Dieser Plan erfordert eine reaktionsschnelle und skalierbare Lösung, die Folgendes erreicht:

1. **Schutz von Daten und Systemen:** Ihre Lösung sollte Ihre MitarbeiterInnen schützen, egal wo und mit welchem Gerät sie arbeiten.
2. **Verbesserung der Ausfallsicherheit bei Cyberangriffen:** Verschiedene Schichten von Sicherheits- und Disaster-Recovery-Funktionen sind wesentliche Komponenten.
3. **Reduzieren der Komplexität von Sicherheit:** Eine schlanke, benutzerfreundliche Lösung trägt zur Steigerung der Compliance bei.

F

Als CIO ist es Ihre Aufgabe, Ihre Unternehmenstechnologien zu stärken und das Vertrauen derer zu gewinnen, die auf sie angewiesen sind. Dazu müssen Sie sich einige wichtige Fragen stellen:

- Deckt die Cybersicherheit Ihres Unternehmens die End-to-End-IT-Umgebung, einschließlich Geräten, Anwendungen und Systemen, ab?
- Welche Sicherheitsmaßnahmen haben Sie für den Fall, dass sich EndnutzerInnen unvorsichtig verhalten? Setzen Sie beispielsweise KI-basierte Optimierungssoftware ein, um die Datenschutzkontrollen zu automatisieren, wenn sich NutzerInnen von ihren Geräten entfernen?
- Hat Ihr Unternehmen die neuen und potenziell größeren Risiken bewertet, die durch zunehmende Remotearbeit entstehen?

Schutz von Daten und Systemen

Die Komplexität und Silos einer verteilten Belegschaft vervielfachen die Sicherheitslücke für Cyberangriffe. Jedes Mal, wenn unternehmenseigene Daten über Clouds und Remotearbeitsumgebungen gesendet werden, sind diese Daten gefährdet.

Diese Sicherheitslücken können durch ein End-to-End-Sicherheitsmodell geschlossen werden, das Silos und Komplexität überwindet, wie z. B. Zero Trust.

Zero Trust ist ein IT-Sicherheitsmodell, das auf der Annahme basiert, dass keine Interaktion vertrauenswürdig ist und daher jede Interaktion überprüft werden muss. Dieses Modell der Authentifizierung bei jedem Schritt kann auf das gesamte Netzwerk, die IT-Infrastruktur, die Software und die Microservices Ihres Unternehmens angewendet werden.

Mit einem mehrschichtigen Zero-Trust-Ansatz wird ein Perimeter um jede Interaktion herum erstellt. Selbst wenn Bedrohungsakteure eine Grenze überschreiten, werden sie nicht in der Lage sein, eine Vertrauensstellung auszunutzen, die auf ihrem aktuellen Zugriff auf das System beruht. Jedes Gateway, das sie passieren möchten, erfordert eine Authentifizierung. Diese Sicherheitsprotokolle, bei denen standardmäßig allem misstraut wird, können dazu beitragen, Ihre Daten, das Vertrauen Ihrer Belegschaft und Ihre vertrauensvollen Beziehungen zu Ihren Kunden zu schützen.

Bevor Sie damit beginnen, die Systeme Ihres Unternehmens zum Schutz von Anwendungen und Daten zu optimieren, sollten Sie die folgenden wichtigen Fragen berücksichtigen:

- Entwickelt sich Ihr allgemeiner Sicherheitsstatus in Richtung eines Zero-Trust-Modells?
- Verfügen Ihre Anbieter und Ihr internes DevOps-Team über geeignete Cybersicherheitsmaßnahmen, um einen sicheren Entwicklungslebenszyklus zu gewährleisten, der die Prozesse schützt, mit denen neue Produkte, Funktionen und Services entwickelt/implementiert werden?
- Ist Ihre aktuelle Sicherheitsfunktion im Nachhinein aufgesetzt oder integriert? Isoliert oder vereinheitlicht? Bedrohungsorientiert oder kontextorientiert?

Der Schutz Ihrer Daten hängt davon ab, wo und wie Ihre Sicherungsdaten gespeichert werden. Bevor Cyberkriminelle Ihre Kerndaten stehlen, werden sie in der Regel versuchen, Ihre Backups anzugreifen.

Verbesserung der Ausfallsicherheit bei Cyberangriffen

Wie man so schön sagt: **„Das Einzige, was noch schwieriger ist als die Planung für den Katastrophenfall ist die Erklärung, warum man nichts getan hat."**

Das Entscheidende bei der Erreichung von Ausfallsicherheit bei Cyberangriffen ist die Erwartung eines Angriffs und die Ergreifung vorausschauender Maßnahmen, um sich so schnell wie möglich mit minimalen finanziellen und betrieblichen Auswirkungen erholen zu können.

Zu diesen Schritten gehört die Durchführung von Simulationen, die Ihre Systeme für die Geschäfts- und Betriebskontinuität und -wiederherstellung sowie Ihre Cybersicherheitsmaßnahmen und die Reaktion des Unternehmens in Schlüsselbereichen wie Rechtsfragen, Krisenmanagement und Kommunikation einem Stresstest unterziehen.

Diese Art von rigorosen Tests kann jedoch zeitaufwändig sein. Eine gemanagte Lösung kann Ihrem Team diese Aufgaben abnehmen und hält es über neue Bedrohungen sowie Trends bei Cyberangriffen auf dem Laufenden. Beispielsweise sucht der Managed Detection and Response-Service nach Bedrohungen und prüft die Reaktionen Ihres Unternehmens für Sie.

Eine weitere wichtige Überlegung ist die Archivierung Ihrer Daten. Das bedeutet, dass Sie wissen müssen, wo und wie Ihre Sicherungsdaten gespeichert sind. Bevor CyberangreiferInnen Ihre Kerndaten stehlen, werden sie in der Regel versuchen, Ihre Backups anzugreifen.

Am besten schützen Sie sich dagegen mit einer isolierten Offlinekopie Ihrer kritischen Systeme. Die Erfahrung der Founders Federal Credit Union (FFCU) ist ein gutes Beispiel dafür, wie und warum dies gelingen kann.

Die FFCU kalkulierte, dass sie im Falle eines Cyberangriffs z. B. mit Ransomware ein Zeitfenster von einer Stunde hätte, um ihre Daten wiederherzustellen und den Betrieb wieder aufzunehmen. Dies veranlasste sie zu einer umfassenden Überarbeitung der Cybersicherheit ihres Rechenzentrums mit besonderem Augenmerk auf eine schnelle Wiederherstellung des Betriebs. Sie implementierten einen Cyber-Recovery-Vault, der sich hinter einer betrieblichen „Air Gap" befindet. Diese trennt ihn von ihrem System, während er gleichzeitig regelmäßig Produktionsdaten synchronisiert. Auf diese Weise kann die FFCU darauf vertrauen, dass ihre Daten immer verfügbar, geschützt und unbeschädigt sind.

Wenn Sie Ihre Ausfallsicherheit bei Cyberangriffen in einer sich entwickelnden Sicherheitslandschaft stärken möchten, sollten Sie die folgenden Fragen berücksichtigen:

- Hat Ihr Unternehmen ermittelt, wie lange der Betrieb im Fall eines Cyberangriffs unterbrochen sein würde?
  - Wenn ja, sind es Minuten, Tage oder Wochen?
- Wann haben Sie das letzte Mal geschäftskritische Workloads und Daten ermittelt, die isoliert geschützt werden sollten?
- Über welche Art von Bedrohungserkennungsfunktionen verfügen Sie?
  - Werden diese intern oder von Dritten gemanagt?
  - Nutzt Ihr Unternehmen eine KI-basierte Musteranomalieerkennung?

Komplexität beeinträchtigt die Sicherheit

Wenn Ihr Sicherheitsteam Lösungen für eine Vielzahl von IT-Infrastrukturkomponenten managt, kann die Komplexität und damit das Risiko schnell steigen. Diese Komplexität führt auch zu höheren Kosten und Ineffizienz in Ihrem regulären Betrieb. Die Suche nach einem Gleichgewicht zwischen diesen beiden Aspekten führt in der Regel zu einem unhaltbaren Kompromiss an beiden Fronten.

Es gibt einen besseren Ansatz für die Skalierung Ihrer Cybersicherheitsoperationen. Mit fortschrittlichen Sicherheitstools, die künstliche Intelligenz (KI) und maschinelles Lernen (ML) nutzen, können Sie Zeit und Ressourcen freisetzen, um eine konsistentere Governance und ein konsequenteres Verhalten zu ermöglichen.

KI-Tools helfen Ihren Lösungen zur Erkennung von Bedrohungen dabei, Anomalien im Netzwerk sowie Verstöße gegen Richtlinien zu erkennen und zu melden, was eine Kaskade von Sicherheitsmaßnahmen auslösen würde. Automatisierte Sicherheit kann auch den Softwareentwicklungscode verbessern. Je weniger Fehler und menschliche Irrtümer, desto weniger Sicherheitslücken.

Um jedoch den maximalen Nutzen aus Ihren Sicherheitstools zu ziehen, müssen diese einfach zu bedienen und zu verwalten sein. Durch die Konsolidierung der Sicherheitsanwendungen und Partner Ihres Unternehmens erhalten Sie mehr Kontrolle und vereinfachen das IT-Management, sodass sich Ihre IT-Teams auf Innovationen konzentrieren können. Managed Services können eine großartige Möglichkeit sein, die neuesten und besten Sicherheitstechnologien zu nutzen und gleichzeitig die internen Teams zu entlasten. Es ist jedoch wichtig, Anbieter nach Möglichkeit sorgfältig auszuwählen und zu rationalisieren. Achten Sie darauf, einen vertrauenswürdigen Partner auszuwählen, der nicht nur Ihre einzigartigen Herausforderungen versteht, sondern auch die Fähigkeiten Ihrer IT-Teams mit Cybersicherheitsservices optimieren kann, damit Sie langfristig effizient bleiben.

Wenn Sie Ihre Arbeitsabläufe rationalisieren möchten, ohne Ihre Abwehrmaßnahmen zu verschlechtern, sollten Sie sich diese Fragen stellen:

- Hat Ihr Unternehmen ausreichend Redundanz bei Sicherheitsfunktionen sichergestellt?
- Verwendet Ihr Unternehmen KI-Tools zur Erkennung, Reaktion und Recovery?
- Überprüft Ihr Unternehmen regelmäßig seine internen und externen Sicherheitsanbieter, um Effektivität und Wert sicherzustellen?

Eine mobile Arbeitswelt erfordert intelligentere Sicherheit

Verteilte Daten, ortsunabhängige Arbeitsmodelle, Multi-Cloud-Umgebungen und As a Service-Beschaffung sorgen für erhebliche Unsicherheit in der modernen Cybersicherheitslandschaft. Menschliches Versagen kann diese Unsicherheit noch verstärken. Als CIO ist es Ihre Aufgabe, dafür zu sorgen, dass Ihre Cybersicherheit all diese Faktoren berücksichtigt.

Ein moderner Ansatz für die Cybersicherheit ist von entscheidender Bedeutung. Ihr Cybersicherheitsansatz muss in der Lage sein, Ihre Daten und Systeme zu schützen, die Auswirkungen von Cyberangriffen zu reduzieren und Cybersicherheitsmaßnahmen effektiv zu skalieren – und all dies bei minimaler zusätzlicher Komplexität.

Dell Technologies unterstützt Sie bei der Planung, dem Schutz, der Erkennung, der Reaktion auf und der Wiederherstellung nach Cyberangriffen, damit sich Ihre Teams und Ressourcen voll und ganz dem widmen können, worauf es ankommt – Ihr Unternehmen voranzubringen.

Weitere Informationen finden Sie unter dell.com/cio.

Weitere Informationen zur Breakthrough-Studie finden Sie unter dell.com/breakthrough.

Weitere Informationen zu unseren Sicherheitslösungen finden Sie hier:
dell.com/en-us/dt/solutions/security/index.htm

Quelle: Basierend auf der „Studie zu bahnbrechenden Erfolgen" von Dell Technologies vom April 2022. Die Feldforschung erfolgte von August bis Oktober 2021. Die Untersuchung und Analyse wurden von Vanson Bourne im Auftrag von Dell Technologies durchgeführt.

Copyright © 2022 Dell Inc. oder deren Tochtergesellschaften. Alle Rechte vorbehalten. Dell Technologies, Dell, EMC, Dell EMC und andere Marken sind Marken von Dell Inc. oder deren Tochtergesellschaften. Alle anderen Marken können Marken ihrer jeweiligen Inhaber sein.

DELL Technologies