okta

Okta Checkliste: So schützen Sie sich vor Ransomware

Wie ein Identity-basierter Zero-Trust-Ansatz Ihr Unternehmen in drei einfachen Schritten vor Ransomware schützt

Weiter

Ransomware ist alles andere als neu. Doch mit dem weltweiten Wechsel hin zu einer hybriden Arbeitswelt, die innerhalb und außerhalb des Perimeters agiert, gewinnt das Thema abermals schlagartig an Bedeutung.

Der **Report „The State of Ransomware 2021“ von Sophos** stellt fest, dass 37 % der Unternehmen dieses Jahr bereits Opfer von Ransomware waren. Die Kosten für die Behebung eines solchen Angriffs haben sich dabei mehr als verdoppelt: von 761.106 Dollar in 2020 auf 1,85 Millionen Dollar in 2021. Was steckt hinter diesem plötzlichen Anstieg?

Robuste Daten-Backup- und Recovery-Prozesse galten früher als probates Mittel, um sich vor Ransomware-Forderungen zu schützen. Man hört zwar immer wieder von Fällen, in denen auch die Backups infiziert wurden, doch diese Szenarien sind eher selten. Die Ransomware-Crews haben aber neue Wege gefunden, um bestehende Security-Maßnahmen zu umgehen und sicherzugehen, dass ihre Mühe belohnt wird.

SOPHOS
Cybersecurity evolved.

Häufig stehlen sie die Daten vor der Verschlüsselung, und drohen bei der Erpressung damit, diese publik zu machen. Wenn das Netzwerk einmal kompromittiert wurde, kann der Zugang zudem über spezialisierte Access-Broker an andere Kriminelle weiterverkauft werden, was eine Vielzahl weiterer Attacken nach sich zieht. Richtet sich ein Ransomware-Angriff gegen die Supply Chain, versuchen die Angreifer mitunter auch, Einfluss auf die Kunden des Opfers zu nehmen, und so den Druck zu erhöhen, die Services zeitnah wiederherzustellen.

Manchmal werden die Informationen über den Angriff auch Börsenmaklern angeboten, die dann Leerverkäufe beauftragen, bevor der Angriff der breiten Öffentlichkeit bekannt wird. Mit Ransomware-as-a-Service steht jetzt zudem auch technologischen Laien gegen eine vergleichsweise kleine Gebühr die Möglichkeit offen, Ransomware-Attacken zu initiieren. Kurz: Ransomware ist eine flexible Waffe im Arsenal der Cyberkriminellen, die unzählige Möglichkeiten bietet, sich am Unglück anderer zu bereichern. Was ist die Lösung?

Es gibt kein Allheilmittel, um Ihr Unternehmen vor Ransomware zu schützen. Doch in diesem Guide verraten wir Ihnen, wie Sie mit einem Identity-basierten Zero-Trust-Ansatz vielen gängigen Angriffen einen Riegel vorschieben.

Schritt 1

Verhindern Sie Ransomware-Angriffe mit einer starken, adaptiven Mehrfaktor-Authentisierung

Auf der Suche nach Schwachstellen im Corporate-Netzwerk haben Kriminelle für gewöhnlich die Qual der Wahl. Schwache Zugangsdaten und Passwörter lassen sich oft mit Credential Stuffing oder Password Spraying knacken und öffnen damit die Tür für Ransomware-Angreifer. Aber auch starke Zugangsdaten und Passwörter sind angreifbar. Viele Opfer lassen sich durch Phishing-Angriffe austricksen und verraten unwissentlich Ihre Zugriffsdaten.

Zum Glück gibt es mit **Adaptive Multi-Factor Authentication** einen wirksamen Weg, um Account-Übernahmen zu verhindern. Adaptive MFA steuert Zugriffe auf der Basis kontextbasierter Access-Policies. Dabei unterscheidet sie zwischen normalen und ungewöhnlichen Verhaltensweisen sowie zwischen Aktivitäten mit geringem und hohem Risiko-Potenzial. Diese sind häufig die ersten Hinweise auf bösartige Aktivitäten.

Adaptive MFA verhindert, dass Ransomware-Crews in das Netzwerk eindringen. Eine holistische Zero-Trust-Architektur schiebt darüber hinaus aber auch der lateralen Bewegung im Netzwerk einen Riegel vor.

Euro Garages

Euro Garages* vereinfachte vor kurzem seine IT-Prozesse und ermöglichte 4.000 Mitarbeitern und 1.000 externen Partnern den reibungslosen, sicheren Zugriff auf alle Anwendungen, die sie für die Arbeit im Homeoffice benötigten. Das Unternehmen wechselte mit Okta Single Sign-on und Adaptive MFA einfach und schnell auf ein Zero-Trust-Modell, das die Daten individuell schützt und den Mitarbeitern die freie Wahl darüber lässt, welches Endgerät sie nutzen möchten. Okta steigerte nachhaltig die Produktivität, da die Mitarbeiter arbeiten können, wo sie wollen – und reduzierte die Zahl der Breaches bei Euro Garages durch ein starkes Identity- & Access-Management auf Null.

*Quelle

Schritt 2

Der schnellste Weg zum Identity-basierten Zero-Trust-Ansatz

Viele Unternehmen haben zu Beginn ihrer Zero-Trust-Journey unterschiedlichste On-Prem- und Cloud-Anwendungen im Einsatz, die nicht miteinander integriert sind. Die IT muss in diesem Fall einen bunten Mix verteilter Identitäten managen, die sich auf unterschiedlichsten Systemen und (Schatten-) Anwendungen befinden.

Die Folge sind heterogene und fragmentierte Access-Umgebungen, die zu neuen Schwachstellen führen, die Angreifer ausnutzen können. Hinzu kommt, dass die Anwender in diesem Szenario multiple Zugangsdaten benötigen – und sich daher allzu oft für unsichere, leicht zu hackende Passwörter entscheiden. Durch die fehlende Transparenz und Kontrolle über die verteilten Identitäten stehen den Angreifern viele Einfallstore offen.

Setzen Sie auf einen Identity-basierten Ansatz. Nutzen Sie IAM als zentrale Kontrollinstanz für User, Geräte, Daten und Netzwerke – und behalten Sie jederzeit den Überblick. „Identity first"-Security ist laut **Gartner** einer der wichtigsten Security-Trends von 2021, weil die Unternehmen damit jederzeit die volle Transparenz und Kontrolle darüber erhalten, welche User auf welche Ressourcen Zugriff haben. Ein „Identity first"-Ansatz stoppt zuverlässig Ransomware-Angriffe über kompromittierte Zugangsdaten, fehlerhaftes Provisioning oder schwache Authentifizierung und stellt die Weichen für Zero Trust:

Schritt 1: Beginnen Sie mit dem Aufbau eines einheitlichen Identity- & Access-Managements (IAM) und eliminieren Sie schwache Passwörter durch die Integration von **Single Sign-on (SSO)** und **Adaptive MFA** beim Zugriff auf wichtige Ressourcen.

Schritt 2: Binden Sie auch die Zugriffe auf weitere Ressourcen wie APIs in das IAM ein und verbessern Sie die Authentifizierung durch kontextbasierte Abfragen und ein breites Set von Faktoren.

Schritt 3: Setzen Sie bei der Authentifizierung auf einen durchgängig risikobasierten Zero-Trust-Ansatz, mit passwortlosem Zugriff und durchgängiger Access-Kontrolle.

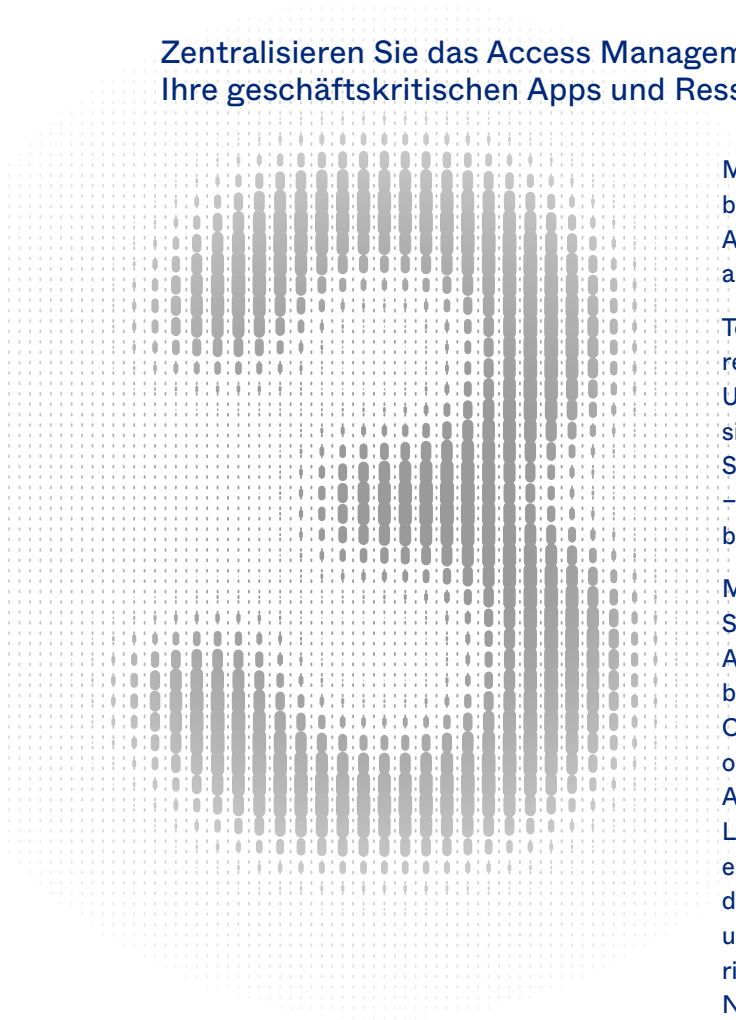
مطارات دبي
DUBAIRPORTS

Okta begleitete **Dubai Airports*** auf der Zero-Trust-Journey und reduzierte die Angriffsfläche des Unternehmens, indem Security-Entscheidungen auf die jeweiligen User und den Kontext des Logins abgestimmt werden. Der „Identity first“-Ansatz schützte die Daten von Dubai Airports auf individueller Ebene und erlaubte den Mitarbeiter flexibel jedes Gerät ihrer Wahl zu nutzen. Dubai Airports‘ 4.000 Mitarbeiter (sowie die 100.000 Mitarbeiter auf dem Campus) können sicher arbeiten, ohne um ihre Daten zu fürchten, seit Okta Adaptive MFA sowohl Cloud- als auch On-Prem-Anwendungen beschützt.

*Quelle

Schritt 3

Zentralisieren Sie das Access Management für Ihre geschäftskritischen Apps und Ressourcen



Multiple Passwörter für verschiedene Apps beeinträchtigen die User-Experience, verlangsamen die Abläufe im IT- und Security-Management, erschweren auch die Authentifizierung und erhöhen das Angriffsrisiko.

Tools wie SSO können die Bedrohung durch Ransomware reduzieren, indem sie alle Apps und Plattformen Ihres Unternehmens durch Single Sign-on schützen. So können sich User schnell authentifizieren, während Ihre IT- und Security-Teams die Zugriffe effizient und sicher managen – und verdächtige Aktivitäten isolieren und angehen, bevor Schaden entsteht.

Mit **Okta Lifecycle Management** verbessern Sie den Schutz Ihres Unternehmens gegen Ransomware-Angriffe. Laut **CRN Report** missbrauchten Hacker beim berüchtigten Ransomware-Angriff auf die Colonial Pipeline einen ruhenden/inaktiven Account ohne Multi-Faktor-Authentifizierung. MFA hätte die Account-Übernahme durch Dritte verhindert, während LCM den Account und/oder seine Privilegien komplett entfernt hätte. LCM automatisiert das Provisioning über den gesamten Joiner-Mover-Leaver-Zyklus hinweg – und gewährt jedem User den richtigen Zugriff auf die richtigen Apps zur richtigen Zeit. So können Hacker Ihr Netzwerk nicht mehr über inaktive Accounts infiltrieren.

Aber schwache Passwörter und inaktive Accounts sind nicht das einzige Einfallstor für Ransomware: Hacker nehmen gezielt Unternehmen mit komplexen, veralteten Architekturen und ungeschützten Integrationen ins Visier. Diese umfangreichen und komplexen Netzwerke bieten Cyberkriminellen eine riesige Angriffsfläche – und diese zu reduzieren, stellt IT-Führungskräfte vor eine enorme Herausforderung.

Das Okta Integration Network bietet Ihrem Unternehmen Tausende von vorgefertigten Integrationen, vermindert mit modernen Protokollen wie OpenID Connect das Risiko unsicherer Passwörter und erlaubt Ihnen, konsistente, dynamische und kontextbasierte Access-Policies für all Ihre Ressourcen durchzusetzen – während Sie Ihren Kunden die beste User-Experience bieten.

Aufsetzend auf Cloud Traffic und Muster der App-Nutzung optimieren Network Security und CASBs die Compliance und den Datenschutz. Security-Analysen gewähren Ihnen eine größere Transparenz in die Cloud-, mobile und On-Prem-Systeme – für eine effiziente Korrelation und Durchsetzung.

So können Ihre Security- und IT-Teams einfach und schnell die neuesten Apps einführen, Ihr User-Management zentralisieren und Ihre Access-Workflows über alle Cloud-, On-Prem- und Mobile-Anwendungen hinweg mit minimalem Aufwand automatisieren.

Vinted

Um die Weichen für das weitere Wachstum zu stellen, benötigte **Vinted*** eine Plattform, die manuelle Aufgaben automatisierte und den Usern eine reibungslose Security bot. Okta implementierte in einem Bruchteil der üblichen Zeit und mit einem deutlich kleineren Budget eine moderne Identity-Lösung, die 95 % der fast 400 Vinted-Apps out-of-the-box via SSO integrierte. Im Zuge der Integration von Okta entdeckte das Projektteam zahlreiche Schatten-Anwendungen sowie doppelte Abonnements und Services, z.B. drei oder vier Apps mit gleicher Funktion. Vinted entschied sich daher, ein eigenes Verzeichnis der Benutzer und Anwendungen auf der Basis von Okta Universal Directory zu erstellen. Damit verfügte das Unternehmen zum ersten Mal über eine zentrale, lückenlose Liste, aus der genau hervorgeht, wer was verwendet – und wie er es verwendet.

*Quelle

okta

Warum Okta?

Die Cyberkriminellen schlafen nicht. Seien Sie den Ransomware-Angreifern daher immer einen Schritt voraus und vertrauen Sie auf einen IDaaS-Provider, der Ihr Unternehmen 24/7 beschützt.

Okta, **die Nummer 1 unter den Plattformanbietern,** wird von führenden Analysten regelmäßig als Leader ausgezeichnet. Mehr als 13.000 Kunden weltweit vertrauen auf die Lösungen von Okta. Im Okta Integration Network ist die branchenweit breiteste Palette an vorgefertigten Out-of-the-Box-Integrationen erhältlich – für mehr als 6.500 Cloud-, On-Prem- und mobile Anwendungen.

Aufsetzend auf unsere erstklassigen, innovativen Identity-Lösungen überzeugt die globale, skalierbare Cloud-Architektur von Okta mit einer durchschnittlichen Laufzeit von 99,99 %, was unsere Plattform **zur vertrauenswürdigsten und zuverlässigsten Lösung im Markt macht.**

Sehen Sie sich die MFA Demo an
Wir zeigen Ihnen, wie Sie mit starker Multi-Factor Authentication Ihre Netzwerk-Security und Ihre Verteidigung gegen Ransomware-Angriffe stärken.

Demo ansehen

Bereit für den Okta Test?
Starten Sie heute Ihren kostenlosen 30-Tage-Test.

Zum kostenlosen Test