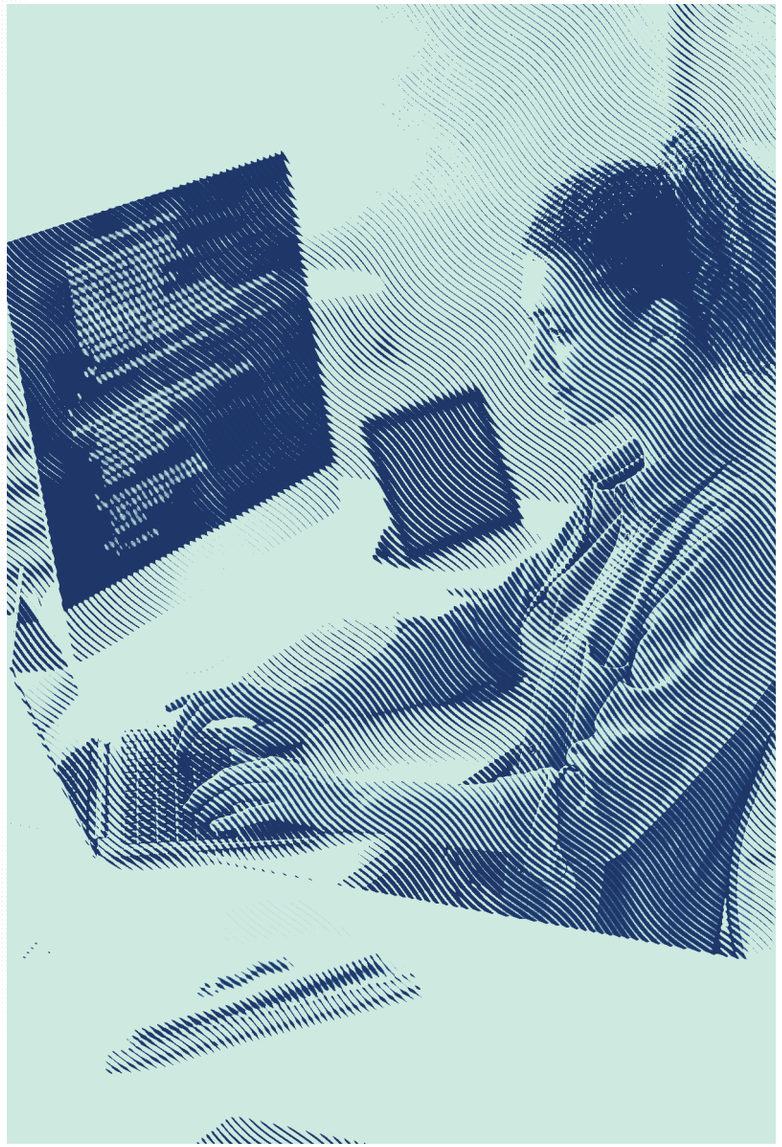
Okta's checklist voor de preventie van ransomware

Drie praktische stappen om uw organisatie tegen ransomware-aanvallen te beschermen met een identity-centrische Zero Trust-benadering tot security

Openen



Ransomware is zeker niet nieuw, maar veel organisaties zijn kwetsbaarder dan ooit tevoren als gevolg van de snelle wereldwijde verschuiving naar het nieuwe werken dat zowel binnen als buiten de perimeter plaatsvindt.

Volgens het rapport **The State of Ransomware 2021 van Sophos** is dit jaar tot nu toe al 37% van de organisaties getroffen door ransomware. Ondertussen zijn de gemiddelde herstelkosten van een ransomware-aanval meer dan verdubbeld, van $ 761.106 in 2020 tot $ 1,85 miljoen in 2021. Maar wat zit er achter deze plotselinge toename?

Men ging er altijd vanuit dat betrouwbare databack-ups en uitgekiende herstelprocedures een goede bescherming boden tegen het betalen van losgeld. Er doen weliswaar enkele nare verhalen de ronde over back-ups die ook zouden zijn geïnfecteerd, maar dat zijn uitzonderingen. Ransomwaregroepen hebben echter nieuwe manieren ontdekt om security-maatregelen te omzeilen en te zorgen dat hun inspanningen worden beloond.

SOPHOS
Cybersecurity evolved.

Data wordt tegenwoordig vaak gestolen vóór de versleuteling, zodat een aanvaller kan dreigen deze te publiceren, als extra aansporing om het losgeld te betalen. Wanneer een aanvaller eenmaal is binnengedrongen, kan de toegang tot het netwerk via access brokers worden verkocht aan andere criminelen. Dat leidt tot nog meer aanvallen die verschillende motieven kunnen hebben. Als een supply chain wordt getroffen door een ransomware-aanval, kan via de klanten van een leverancier nog meer druk op het slachtoffer worden uitgeoefend om de service snel te herstellen.

Voorkennis van een aanval kan ook worden verkocht aan financiële tussenpersonen die vervolgens kunnen speculeren op koersdalingen voordat het probleem bekend wordt op de markt. Specifieke technische ervaring is tegenwoordig ook niet meer nodig, omdat complexe kwaadaardige technologie via Ransomware-as-a-Service voor een relatief kleine vergoeding aan een steeds grotere criminele doelgroep beschikbaar wordt gesteld. Kortom, we hebben te maken met een slagvaardige en flexibele criminele bedrijfstak die veel wisselende manieren tot zijn beschikking heeft om geld te verdienen aan de technische ellende van anderen. Dus wat is de oplossing?

Uw organisatie kan helaas niet met één magische oplossing worden beschermd tegen ransomware-aanvallen. In deze handleiding onderzoeken we daarom hoe een op Zero Trust gebaseerde, identity-gedreven securitystrategie het aantal datalekken kan terugdringen dat vaak aan deze aanvallen ten grondslag ligt.

okta

Stap 1

Neutraliseer ransomware-aanvallen met krachtige Adaptive Multi-Factor Authentication

Cybercriminelen hebben een zeer ruime keuze als het gaat om het vinden van kwetsbaarheden in zakelijke IT-netwerken. Zwakke gebruikersnamen en wachtwoorden kunnen vaak eenvoudig worden gehackt via credential stuffing of password spraying en vormen dus een gemakkelijk toegangspunt voor ransomware-aanvallers. Maar ook sterke gebruikersnamen en wachtwoorden zijn zeer kwetsbaar, met name voor intelligente phishing-aanvallen waarbij slachtoffers op sluwe wijze hun inloggegevens worden ontfutseld.

Gelukkig is **Adaptive Multi-Factor Authentication** een van de meest effectieve manieren om account takeovers te voorkomen. Via adaptive MFA worden toegangsrechten verleend op basis van contextafhankelijke access policies om onderscheid te maken tussen normaal en abnormaal gedrag en tussen gebruikersacties met een laag en een hoog risico. Signalen over abnormaal gedrag en acties met een hoog risico zijn vaak de eerste indicatie van kwaadaardige activiteit.

Adaptive MFA kan voorkomen dat ransomware-aanvallers zich toegang verschaffen tot een systeem, maar een holistische Zero Trust-architectuur biedt bescherming tegen laterale bewegingen van aanvallers die het netwerk al zijn binnengedrongen.

okta

Euro Garages* heeft onlangs een nieuwe strategie uitgestippeld om de IT-processen te vereenvoudigen en zijn 4000 werknemers en 1000 externe partners frictieloze en veilige toegang te bieden tot alle cruciale applicaties die ze nodig hebben om remote te kunnen werken. Door gebruik te maken van Okta Single Sign-On en Adaptive MFA kon de organisatie snel een Zero Trust-securitymodel implementeren. Dit model beschermt niet alleen data op individueel niveau, maar biedt werknemers ook de flexibiliteit om hun taken op elk gewenst device uit te voeren. De mogelijkheden die Okta biedt om de allerbeste identity en access management-practices toe te passen heeft grote voordelen opgeleverd. Zo is de productiviteit verbeterd, hebben werknemers de vrijheid om te werken waar het hen het beste uitkomt en is Euro Garages erin geslaagd het aantal datalekken tot nul terug te brengen.

*Bron

Stap 2

Implementeer uw identity-centrische Zero Trust-architectuur sneller

Veel organisaties beginnen hun Zero Trust-journey met een verscheidenheid aan on-prem en cloudapplicaties die volledig los van elkaar staan. Het IT-team moet dan ook vaak verschillende identities uit veel verschillende systemen beheren, om nog maar niet te spreken over de vele applicaties en services die worden gebruikt zonder dat de IT hiervan op de hoogte is.

Hierdoor ontstaan er problemen met de toegangscontrole, die op hun beurt leiden tot een grotere fragmentatie en meer kwetsbaarheden. Allemaal ontwikkelingen waar ransomware-aanvallers maar al te graag gebruik van maken. Bovendien hebben eindgebruikers vaak meerdere (en waarschijnlijk onveilige) gebruikersnamen en wachtwoorden nodig, die eenvoudig te hacken zijn. Zonder inzicht en zeggenschap over deze gefragmenteerde identities, zitten IT- en securityteams opgescheept met grote gaten in de beveiliging, waarvan aanvallers gebruik kunnen maken om eenvoudig toegang tot individuele systemen te kunnen krijgen.

Als uw organisatie echter besluit identity als de nieuwe perimeter te gebruiken, wordt IAM het centrale controlepunt voor alle gebruikers, devices, data en netwerken. Volgens **Gartner** is deze identity-gedreven security een van de belangrijkste trends van 2021 op het gebied van security en risico, omdat dit organisaties meer inzicht en controle geeft over welke gebruikers toegang tot welke resources hebben. Door een identity-gedreven securitymodel te adopteren kan uw organisatie het aantal ransomware-aanvallen terugdringen die het gevolg zijn van gehackte inloggegevens, onjuiste provisioning of onjuiste authenticatie. De implementatie van Zero Trust kan in de volgende fasen worden verdeeld:

In fase 1 begint uw organisatie met het bouwen van een gecombineerd Identity Access Management (IAM)-ecosysteem en maakt een einde aan slechte wachtwoordgewoonten door **Single Sign-On (SSO)** en **Adaptive MFA** te implementeren, zodat werknemers op veilige wijze toegang tot belangrijke resources kunnen krijgen.

In fase 2 past uw organisatie aanvullende best practices voor security toe door de toegangscontroles uit te breiden naar andere resources (zoals API's) en door gebruik te maken van essentiële context en verschillende factoren om authenticatiebeslissingen te ondersteunen.

In fase 3 heeft u met succes een volledig op risico gebaseerde authenticatie-benadering tot Zero Trust geadopteerd, inclusief oplossingen voor passwordless authenticatie en continue toegang.

okta

CASESTUDY

مطارات دبي
DUBAIRPORTS

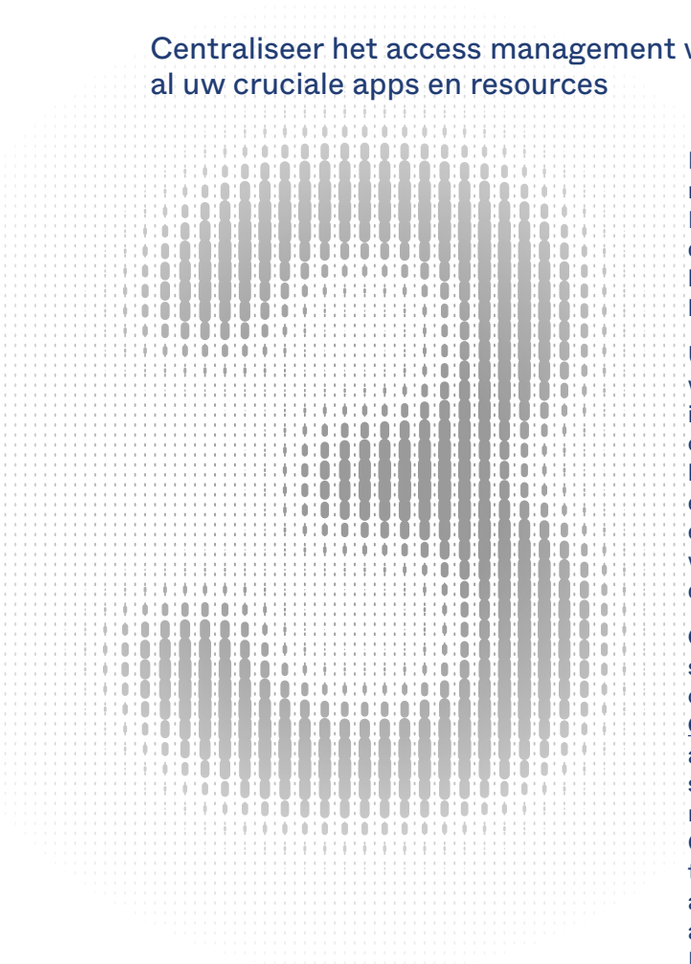
Okta heeft **Dubai Airports*** geholpen om de eerste stappen te zetten naar een Zero Trust-security-strategie en de aanvalsmogelijkheden tot een minimum te beperken, onder andere door security-beslissingen te baseren op individuele gebruikers en de context van hun toegangsverzoeken. Dankzij deze identity-gedreven Zero Trust-benadering kon Dubai Airports zijn data op individueel niveau beschermen en tegelijk zijn werknemers de flexibiliteit bieden om elk gewenst device te gebruiken. Nu zowel de cloudapps als de on-prem apps door Okta Adaptive MFA worden beschermd, kunnen de 4000 werknemers van Dubai Airports en de 100.000 mensen die op de campus werken hun taken veilig uitvoeren zonder het risico te lopen dat hun data aan bedreigingen van buiten worden blootgesteld.

*Bron

okta

Stap 3

Centraliseer het access management voor al uw cruciale apps en resources



Het onthouden van meerdere wachtwoorden voor meerdere apps brengt veel nadelen met zich mee. Het doet afbreuk aan de user experience, belemmert de activiteiten van IT- en securitymanagers, bemoeilijkt het authenticatieproces en verhoogt het risico van blootstelling aan derden.

Uw organisatie kan veel ransomwarebedreigingen voorkomen door een tool zoals Single Sign-On (SSO) te implementeren, zodat u met één veilige, gecentraliseerde oplossing de toegang tot al uw apps en platforms kunt beheren. Hierdoor kunnen gebruikers snel authenticeren en kunnen uw IT- en securityteams de gebruikerstoegang efficiënter en veiliger beheren, onder andere door verdachte activiteiten te isoleren en op te lossen voordat deze de kans krijgen zich verder te verspreiden.

Okta Lifecycle Management kan ook een grote rol spelen in het versterken van de verdediging van uw organisatie tegen ransomware-aanvallers. Volgens dit **CRN-rapport** konden hackers de beruchte ransomware-aanval op Colonial Pipeline in de VS uitvoeren door een slapend of inactief account te infiltreren dat niet met multi-factor authenticatie was beschermd. Met MFA had Colonial Pipeline kunnen voorkomen dat derden toegang tot het account konden krijgen. Maar met LCM zou het account, inclusief de bijbehorende toegangsrechten, al volledig zijn verwijderd. Door de provisioning met LCM te automatiseren tijdens elke stap in de joiner/mover/leaver-cyclus, krijgen gebruikers uitsluitend op het juiste moment de juiste toegang tot de juiste apps. Op deze manier kunnen slapende accounts niet meer door hackers worden gebruikt om controle over uw IT-netwerk te krijgen.

Naast zwakke wachtwoorden en slapende accounts richten ransomware-aanvallers hun pijlen vooral op organisaties met zichtbaar complexe legacy architecturen en slecht werkende integraties. Het terugdringen van de aanvalsmogelijkheden van deze grote complexe netwerken kan echter een enorm probleem zijn voor IT-managers en leidt bovendien vaak tot veel nieuwe kwetsbaarheden die door cybercriminelen kunnen worden misbruikt.

Het Okta Integration Network geeft uw organisatie toegang tot duizenden pre-built integraties en moderne protocollen (zoals OpenID Connect) waarmee het risico van een wildgroei aan wachtwoorden kan worden beperkt. Okta kan u helpen consistente, dynamische en op context gebaseerde access policies voor alle resources in te stellen en tegelijkertijd de user experience te verbeteren.

Netwerkbeveiligings- en CASB-oplossingen letten daarnaast op patronen in het cloudverkeer en het applicatiegebruik om de compliance te verbeteren, de beveiliging tegen bedreigingen aan te scherpen en dataverlies te voorkomen. En met security analytics kunt u uw inzicht in mobiele, on-prem en cloudsystemen uitbreiden om de correlatie en handhaving naar een hoger niveau te tillen.

Op deze manier kunnen uw IT- en securityteams snel en eenvoudig de nieuwste apps adopteren, uw user management centraliseren en de toegang tot workflows automatiseren voor alle mobiele, on-prem en cloudapplicaties.

okta

Vinted

Vinted* had een groeistrategie op de lange termijn uitgestippeld en was op zoek naar een platform dat handmatige taken kon automatiseren en de security kon verbeteren zonder de frictie voor de gebruikers te verhogen. Okta bood kant-en-klare SSO-integraties voor 95% van de 394 apps van Vinted. Hierdoor kon de organisatie veel sneller dan verwacht een moderne identity-oplossing naar het hele netwerk uitrollen tegen een fractie van de kosten die hier normaal mee gemoeid zijn. Het gemak van de integratie met Okta bracht ook nog iets anders aan het licht: Vinted bleek een grote hoeveelheid shadow-IT te hebben, zoals dubbele abonnementen en services, en er waren drie of vier apps die in wezen precies hetzelfde deden. Vinted besloot mede daarom een eigen directory met gebruikers en applicaties te maken met behulp van Okta's Universal Directory. Voor het eerst beschikte de organisatie daarmee over een gecentraliseerde, allesomvattende lijst waarop exact te zien is wie hun applicaties gebruikt en hoe deze worden gebruikt.

*Bron

okta

Waarom Okta kiezen?

Cybercriminelen slapen nooit. Daarom is het investeren in een IDaaS-provider die uw organisatie dag en nacht kan beschermen van essentieel belang om voorop te blijven lopen en ransomware op afstand te houden.

Okta is **'s werelds grootste identityplatform-provider** die consistent als leider wordt uitgeroepen door bekende onderzoeksbureaus en wordt vertrouwd door ruim 13.000 klanten over de hele wereld. Het Okta Integration Network omvat meer dan 6500 kant-en-klare integraties voor mobiele, on-prem en cloudapps en biedt daarmee de grootste verscheidenheid aan pre-built applicatie-integraties van de hele sector.

Naast de elite suite met geavanceerde identity-producten beschikt Okta over een wereldwijde schaalbare cloudarchitectuur met een gemiddelde uptime van 99,99%. Dat betekent dat Okta's identityplatform een van **de meest betrouwbare oplossingen van de sector is.**

Bekijk de MFA-demo
Bekijk deze exclusieve demo en ontdek hoe u krachtige Multi-Factor Authentication kunt implementeren om uw netwerksecurity te verbeteren en uw bescherming tegen ransomware te versterken.

Demo bekijken

Klaar om Okta te proberen?
Start vandaag nog een kosteloze trial van 30 dagen.

Trial starten