Microsoft

Zes stappen voor een holistische beveiligingsstrategie

Deze informatie is voor jou

als je een Chief Information Security Officer of een IT-beveiligingsleider bent die:

- Een snelle no-nonsense handleiding nodig heeft voor een algemene beveiligingsstrategie.
- Op de hoogte wil blijven van de nieuwste beveiligingspraktijken.

Geschatte leestijd: < 9 minuten

Inhoud

De uitdaging aangaan

Organisaties beschouwen het beveiligen van data en systemen als een topprioriteit. Maar deze uitdaging het hoofd bieden wordt elke dag moeilijker nu de aanvallen geavanceerder worden, medewerkers meer verschillende apparaten en applicaties gebruiken en de data op een hoop manieren je bedrijf in- en uitgaat. En omdat massaal wordt overgestapt op extern werken, loopt je beveiliging nog groter gevaar.

Leiders moeten het evenwicht zien te vinden tussen deze uitdagingen en de noodzaak om samen te werken, te innoveren en een bedrijf te laten groeien. Je hebt een veelzijdige beveiligingsbenadering nodig waarbij voortdurend alle eindpunten worden beschermd, vroegtijdige tekenen van een schending worden gedetecteerd en wordt gereageerd voordat er schade optreedt. En hoe sterk je verdediging ook is, preventieve maatregelen zijn niet langer voldoende. Je moet tevens een 'assume breach'-houding aannemen die detectie- en responsmaatregelen omvat.

Moderne Chief Information Security Officers (CISO's) hebben agile beveiligingsframeworks nodig die digitale transformatie mogelijk maken en die worden ondersteund door holistische strategieën die zijn ingebed in technologieën, processen en trainingsprogramma's. Hoewel dit allemaal beschikbaar is voor on-premises oplossingen, staat het onomstotelijk vast dat een overstap naar de cloud onmiddellijk de beveiligingsmogelijkheden van je organisatie verbetert.

> **Met dit eBook delen we de zes best practices van CISO's die hun zakelijke succes hebben te danken aan beveiliging. Deze best practices zijn van toepassing op een on-premises scenario, maar zijn veel gemakkelijker te realiseren in een cloudscenario.**

1. Gebruik geïntegreerde beveiligingsproducten om snel te kunnen reageren

75

Het aantal beveiligingsproducten dat een organisatie van gemiddelde grootte gebruikt.[1]

Bedreigingsspelers hebben zich sterk ontwikkeld sinds de 'smash-and-grab'-aanvallen om systemen binnen te dringen in de hoop op een continue, langdurige aanwezigheid. Aanvallers maken tegenwoordig gebruik van een gevarieerd aanbod aan vectoren en een steeds geavanceerder scala aan tools en technieken: het stelen van referenties, het installeren van malware die zichzelf wist om detectie te voorkomen, het aanpassen van interne processen en het omleiden van netwerkdata, scams via social engineering, en zelfs het targeten van mobiele telefoons en privéapparaten van medewerkers.

Organisaties implementeren meer en meer beveiligingstools om deze bedreigingen het hoofd te bieden. Hoewel deze oplossingen bedoeld zijn voor het wegnemen van specifieke problemen, is er zelden sprake van interactie tussen de oplossingen. In veel gevallen worden eigen dashboards, consoles en logboeken gebruikt. Integratie is lastig en daarom wordt het ook moeilijk om een overkoepelend overzicht te krijgen en bedreigingen snel van een prioriteit te kunnen voorzien. De uitdaging wordt nog groter wanneer we te maken hebben met zowel cloud- als on-premises resources. Het gevolg is dat het soms meer dan 140 dagen kan duren voordat een bedreiging wordt ontdekt.[2]

[1] "Symantec Introduces New Era of Advanced Threat Protection", Businesswire, oktober 2015.

[2] "Threat Landscape: By the Numbers". Mandiant, A FireEye Company, 2016.

Probeer dit eens

Omdat snelle detectie en respons belangrijker worden, zijn deze best practices ontstaan:

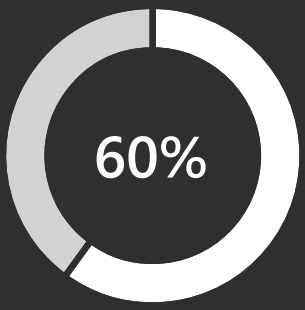
- Krijg een holistisch beeld van de beveiliging voor je hele netwerk, inclusief cloud- en hybride omgevingen.
- Bouw een ecosysteem van beveiligingsproducten en -platforms die met elkaar kunnen worden geïntegreerd en die je inzichten bieden.
- Ga partnerschappen aan met technologieleveranciers die samenwerken en informatie delen in de beveiligingsindustrie.

Belangrijkste inzichten

Door het gebrek aan integratie tussen beveiligingsproducten wordt het voor beveiligingsteams lastig om bedreigingen snel vast te stellen en op een holistische manier aan te pakken.

Zoek producten die qua ontwerp zijn bedoeld voor integratie met andere producten.

2. Beheer toegang via identiteit en niet endpoints



van alle inbreuken is afkomstig van een gehackt of geïnfecteerd endpoint.[3]

Een datalek kan enorme kosten tot gevolg hebben. Voldoende beveiligingscontroles invoeren om inzicht te krijgen in bedreigingen en aanvallen is één manier om de hoge kosten te bestrijden. Maar beveiligingsteams moeten ook consumentgerichte IT ondersteunen, waarbij medewerkers niet langer uitsluitend werken op door het bedrijf verstrekte apparaten die aan strakke regels gebonden zijn en verwachten om overal te kunnen werken, op elk apparaat of elk platform, ongeacht of de IT-afdeling van het bedrijf daarvoor goedkeuring heeft gegeven.

In deze wereld wordt toegang via op identiteiten gebaseerde beveiligingsstrategieën gekoppeld aan identiteit en niet aan apparaten. Pas controles toe op basis van rol en behoefte, ongeacht hoe de gebruiker verbinding maakt. Deze focus op de verificatie en het beheer van gebruikers op het moment dat ze toegang krijgen tot bedrijfsmiddelen, stelt organisaties ook in staat om hun data te beschermen, ongeacht waar deze wordt opgeslagen, benaderd of gedeeld.

[3] "Top Five Security Threats Facing Your Business and How To Respond", Microsoft Secure Blog, oktober 2016.

Probeer dit eens

Als je overstapt van een beveiligingsstrategie die alleen op endpoints steunt, krijg je een robuustere aanpak. Deze tools kunnen je helpen:

- **IAM-oplossingen (Identity and Access Management)** en **beheer van mobiele applicaties met DLP-oplossingen (Data Loss Prevention)**. Beide helpen het risico te verlagen door de toegang tot applicaties en data in bedrijfsresources en in de cloud te beschermen. IAM kan ervoor zorgen dat medewerkers voldoende hebben aan één identiteit voor toegang tot cloud- en on-premises resources. Cloudgebaseerde IAM-systemen kunnen ook gebruikmaken van beveiligingsdata en -analyse van de technologieaanbieder voor een betere detectie van afwijkende aanmeldingspogingen, om daar vervolgens automatisch op te reageren.
- **Multi-Factor Authentication (MFA)** biedt nog een beschermingslaag, waarbij een gebruiker iets moet overleggen dat ze weten (hun wachtwoord) en iets dat ze hebben (secundaire verificatie via een apparaat, vingerafdruk of gezichtsherkenning). Andere robuuste tactieken zijn toegang op basis van risiconiveau van de gebruiker, het apparaat, de applicatie en zelfs de locatie. Deze voorzieningen maken het mogelijk om gebruikers in realtime toe te staan, te blokkeren of om MFA te vragen op basis van het ingestelde beleid, zodat organisaties in feite de beveiliging bij hun eigen voordeur kunnen verbeteren.

Belangrijkste inzichten

Een op identiteit gebaseerde beveiligingsstrategie verlegt de focus van het bewaken van endpoints naar het beheren van gebruikers die bedrijfsdata willen raadplegen.

Meer robuuste endpointbescherming biedt inzicht in bestrijdingstechnieken na een inbreuk.

3. Voer een Zero Trust-model in om bedreigingen te verslaan

17.000
malwarewaarschuwingen

Een organisatie van gemiddelde grootte moet deze wekelijks doorpluizen.[4]

Hackers weten dat elke organisatie meerdere toegangspunten heeft. Ze maken gebruik van phishing-scams, malware- en spyware-aanvallen, zwakke plekken in browsers en software, toegang via kwijtgeraakte en gestolen apparaten, social engineering en andere tactieken om de beveiliging te omzeilen. Bedrijven moeten constant op hun hoede zijn om goed zicht te houden op reeds bekende bedreigingen en zich bewust te zijn van nieuwe beveiligingsproblemen.

Sommige tools kunnen helpen bij het realiseren van continue beveiliging, maar een bredere aanpak is zinvoller. Bij traditionele tools ligt de focus op preventie, maar dat is niet meer voldoende. Organisaties moeten ervan uitgaan dat er al een inbreuk heeft plaatsgevonden of dat er binnenkort een zal plaatsvinden. Dit wordt Zero Trust genoemd. Vervolgens moeten ze manieren vinden om de tijd die nodig is om de inbreuk op te sporen en te herstellen aanzienlijk te verkorten.

[4] "The Cost of Malware Containment". Ponemon Institute, januari 2015.

Probeer dit eens

Word een geavanceerde beveiligingsexpert. Bedreigingen voorblijven kan betekenen dat je terugkijkt om te leren van eerdere incidenten en activiteiten, en de stappen die hackers hebben ondernomen.

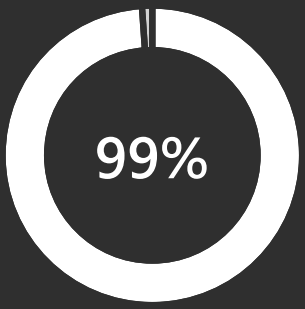
- Veel beveiligingsapplicaties maken gebruik van ingebouwde analytics- en machine learning-mogelijkheden om te analyseren hoe een hacker toegang heeft verkregen. Meer geavanceerde beveiligings- en analyticsoplossingen gebruiken deze inzichten om automatisch actie te ondernemen om vergelijkbare inbreuken te voorkomen en hierop te reageren, waardoor de situatie aanzienlijk sneller kan worden opgelost.
- Deze oplossingen zijn gebaseerd op een enorme omvang en diepgang van signalen en intelligentie. Gecombineerd met de ervaring en kennis van menselijke experts kunnen deze oplossingen krachtige tools zijn tegen snel veranderende bedreigingsspelers.

Belangrijkste inzichten

Cloudapplicaties ondersteunen een Zero Trust-model beter dan oudere applicaties.

Oudere applicaties moet je moderniseren als je er voorwaardelijke toegang op basis van de identiteit op wilt toepassen.

4. Stap veilig over naar de cloud



van de fouten in de cloudbeveiliging zijn, tussen nu en 2025, de schuld van de klant.[5]

Elke organisatie bevindt zich op een ander punt in de transitie naar de cloud. Compliancevereisten, lokale regelgeving en andere migratieproblemen zorgen dat niet elke organisatie er klaar voor is om belangrijke workloads over te zetten naar de cloud. Hybride cloudstrategieën vormen een manier waarop organisaties een zachte overstap naar de cloud kunnen maken, waarbij sommige workloads on-premises worden gehouden en andere worden verplaatst.

Cloudservicemodellen zijn van invloed op de manier waarop serviceproviders en klanten verantwoordelijkheden delen. Dit probleem gaat spelen voor CISO's als ze aan de slag gaan met het vinden van een compromis tussen de gecontroleerde voordelen van on-premises oplossingen en de betere beveiliging van cloudleveranciers.

De vuistregel voor cloudbeveiliging is dat het een gedeelde verantwoordelijkheid is. Cloudproviders moeten beschikken over state-of-the-art beveiliging en encryptie, maar klanten moeten ervoor zorgen dat de services die ze afnemen ook in de praktijk veilig zijn en dat ze vereist beveiligingsbeleid toepassen op hun nieuwe cloudresources.

[5] "Is the Cloud Secure", Gartner, oktober 2019.

Probeer dit eens

Stel de juiste vragen. Bij het beoordelen van cloudproviders kies je niet alleen een service, maar kies je ook aan wie je je data wilt toevertrouwen. Cruciale vragen over beveiliging en toegangsbeheer die je moet stellen zijn onder andere:

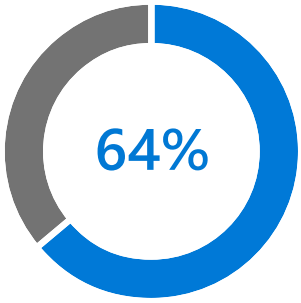
- Wordt onze data beschermd door sterke beveiliging en state-of-the-art technologie?
- Heb je privacy by design ingebouwd en kun je toegang tot onze data in onze enterprise cloud bieden?
- Wat voor soort investeringen heb je gedaan in robuuste en innovatieve complianceprocessen om onze organisatie te helpen voldoen aan de compliancebehoeften?
- Waar wordt onze data opgeslagen, wie heeft er toegang toe en waarom?
- Laat je jaarlijks externe evaluaties uitvoeren om te controleren of aan de beveiligings- en compliancenormen wordt voldaan?
- Verwerp je aanvragen voor openbaarmaking van persoonsgegevens van klanten die niet wettelijk bindend zijn?
- Voldoe je aan de compliance- en regelgevingsnormen van verschillende landen en locaties, en zo ja, welke?

Belangrijkste inzichten

Let er bij de evaluatie van cloudserviceproviders op dat ze zich houden aan internationale standaarden.

Zoek leveranciers die gedetailleerde informatie publiceren over hoe ze hun services exploiteren en data verwerken.

5. Verkrijg een goed inzicht in schaduw-IT



van de medewerkers heeft ten minste één account gemaakt (zich aanmelden voor een website of app voor het werk) zonder de IT-afdeling hierbij te betrekken.[6]

Wanneer een medewerker een cloudaccount maakt zonder dat een bedrijf daarvoor toestemming heeft gegeven of hiervan op de hoogte is, wordt dit schaduw-IT genoemd. De accounts lijken vrij onschadelijk: een tool om bijvoorbeeld de grammatica van schriftelijke tekst te corrigeren. Maar deze accounts creëren zelfs in de strikste beveiligingsconfiguraties kwetsbaarheden.

Mensen accepteren vaak Algemene voorwaarden zonder ze te lezen en zonder volledig te begrijpen waartoe ze toegang verlenen. Traditionele oplossingen voor netwerkbeveiliging zijn niet ontworpen voor het beschermen van data in SaaS-apps en kunnen IT geen inzicht geven in hoe medewerkers de cloud gebruiken.

Uiteindelijk willen we de motivaties achter schaduw-IT niet onderdrukken. Mensen en teams toestemming geven om de cloudapplicaties te gebruiken die het meest geschikt zijn voor hun type werk, stimuleert de productiviteit en innovatie. Het verkrijgen van inzicht in, controle over en beveiliging tegen bedreigingen voor schaduw-SaaS-apps is de eerste stap op weg naar het beheren van risico en het faciliteren van de digitale transformatie die al is gestart binnen je bedrijf.

[6] "New research reveals risks of shadow IT", 1password, februari 2020.

Probeer dit eens

Verkrijg alle vereiste informatie. Cloud Access Security Brokers (CASB's) kunnen organisaties helpen om een gedetailleerd beeld te verkrijgen van de manier waarop hun medewerkers de cloud gebruiken.

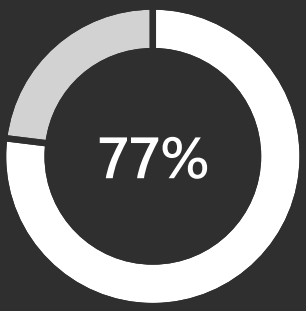
- Welke cloudapps worden door werknemers gebruikt?
- Welk risico vormen deze apps voor de organisatie?
- Hoe worden deze applicaties benaderd?
- Wat voor soort data wordt verzonden naar en gedeeld vanuit deze applicaties?
- Hoe ziet het upload-/downloadverkeer eruit?
- Zijn er afwijkingen in het gedrag van gebruikers, zoals onmogelijke reizen, mislukte aanmeldingspogingen of verdachte IP-adressen?

Belangrijkste inzichten

Cloud Access Security Brokers (CASB's) kunnen een gedetailleerd beeld geven van hoe medewerkers de cloud gebruiken.

Met een betere zichtbaarheid kun je vervolgens beleid instellen om te traceren en bepalen hoe medewerkers deze apps gebruiken.

6. Maak bescherming en productiviteit naadloos



van de CISO's zegt het gevoel te hebben klem te zitten tussen de keuze om mensen vrij te laten werken of het bedrijf veilig te houden.[7]

Je bent veel vaker de controle over data kwijt nu medewerkers, partners en klanten de data delen. Deze trend is goed voor de productiviteit en innovatie, maar kan ingrijpende gevolgen hebben als zeer vertrouwelijke data in de verkeerde handen terechtkomen. Beveiligingsmanagers zijn verantwoordelijk voor het beheren en beveiligen van data die wordt opgeslagen op verschillende locaties en die grensoverschrijdend wordt gedeeld, in compliance met de regelgeving.

Medewerkers hebben al snel genoeg van omslachtige procedures en zullen dan ook op zoek gaan naar manieren om de beveiliging te omzeilen. Classificatie en encryptie van data zijn de beste manieren om data veilig te houden en tegelijkertijd productief gebruik en delen van informatie mogelijk te maken. Je kunt menselijke fouten voorkomen door dataclassificatie te automatiseren. Tools kunnen de context van data begrijpen, zoals creditcardnummers binnen een bestand, of de gevoeligheid van data, gebaseerd op oorsprong. Als labels zijn toegevoegd, kan vertrouwelijke data automatisch worden voorzien van visuele markeringen zoals kopteksten, voetteksten en watermerken, evenals van beveiliging via encryptie, verificatie en gebruiksrechten.

[7] "IT security hindering productivity and innovation, survey shows", ComputerWeekly.com, oktober 2017.

Probeer dit eens

Zorg dat je vertrouwd raakt met de details. Beveiligingsteams moeten de activiteiten kunnen bijhouden die plaatsvindt voor gedeelde bestanden met zeer vertrouwelijke informatie of met een zeer grote impact op het bedrijf, en indien nodig de toegang kunnen intrekken.

- Deze permanente beveiliging is gekoppeld aan de data en de data wordt dus altijd beveiligd, ongeacht waar deze wordt opgeslagen of met wie de data wordt gedeeld.
- Een identiteitsbeheersysteem vermindert de last van het bijhouden van zeer vertrouwelijke bestanden.

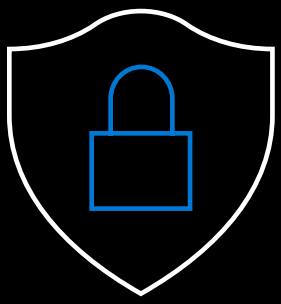
Belangrijkste inzichten

Beveiliging op dataniveau is de verantwoordelijkheid van iedereen.

De classificatie en labeling van data moet plaatsvinden tijdens het aanmaken van de data, en beveiligingsteams moeten activiteiten voor bestanden kunnen monitoren en snel actie ondernemen.

Microsoft

Conclusie



De veelzijdige aard van cyberbedreigingen betekent dat het oplossen van slechts een paar beveiligingsproblemen niet meer voldoende is. De beveiligingsbehoeften van elk bedrijf zijn uniek, maar bedrijven hebben te maken met dezelfde uitdagingen en delen dezelfde verantwoordelijkheid als het gaat om het beschermen van hun data, mensen en systemen zonder dat dit ten koste gaat van innovatie en groei. Je hebt behoefte aan agile beveiligingsframeworks die digitale transformatie bevorderen en steunen, ondersteund door holistische beveiligingsstrategieën die zijn ingebed in technologieën, processen en trainingsprogramma's.

Als je nog niet hebt overwogen om naar de cloud over te stappen, is nu hét moment om de uitgebreide beveiligingsmogelijkheden te verkennen die je er kunt vinden. Microsoft 365 biedt een complete, intelligente oplossing voor bedrijven van elke omvang die jouw digitale transformatie ondersteunt met beveiligings- en compliancevoorzieningen die op elk niveau standaard aanwezig zijn.

Je kunt meer te weten komen in deze gratis uitgebreide webinarserie.

Bekijk de serie >