Microsoft

6 trin til at opbygge en holistisk sikkerhedsstrategi

Disse oplysninger er til dig,

hvis du er sikkerhedschef eller IT-sikkerhedschef, der:

- Har brug for en hurtig og enkel guide til generelle sikkerhedsstrategier.
- Ønsker at holde sig orienteret om seneste praksis inden for sikkerhed.

Anslået læsetid: under 9 minutter

Indhold

Tag udfordringen op

Sikring af data og systemer har højeste prioritet for organisationer. Men det bliver hele tiden sværere at leve op til denne udfordring, i takt med at angrebene bliver mere sofistikerede, medarbejderne bruger en lang række forskellige enheder og programmer, og data flyder ind og ud af virksomheden på flere og flere måder. Det store skift til fjernarbejde har skabt endnu større trusler for sikkerheden.

Lederne skal balancere disse udfordringer med behovet for at samarbejde, innovere og udvikle en virksomhed. Du har brug for en mangefacetteret sikkerhedstilgang, der konstant beskytter alle endepunkter, opdager tidlige tegn på et brud og reagerer, før skaden opstår. Og ligegyldigt hvor stærkt dit forsvar er, er de sædvanlige forebyggende foranstaltninger ikke længere tilstrækkelige. Du må altid "tro det værste" i forhold til registrering og håndtering af angreb.

Nutidens CISO'er (Chief Information Security Officers) har brug for fleksible sikkerhedsstrukturer, som muliggør digital transformation og understøttes af integrerede holistiske strategier for teknologier, processer og uddannelsesprogrammer. Selv om alt dette er til rådighed for on-premises-løsninger, giver skiftet til skyen i virkeligheden en omgående forbedring af sikkerhedsmulighederne i hele organisationen.

Denne e-bog giver dig de seks bedste praksisser fra CISO'er, der har gjort sikkerhed til hjørnestenen i deres forretningssucces. Disse bedste praksisser er gældende for et on-premises-scenarie, men er uendeligt meget nemmere at opnå i et cloud-scenarie.

1. Brug integrerede sikkerhedsprodukter for at få hurtig responstid

75

Antal sikkerhedsprodukter, som en gennemsnitlig stor organisation bruger.[1]

Truslerne har udviklet sig fra hurtige angreb, der kompromitterer systemer indefra i håbet om at kunne udnytte dets data over længere tid. Angriberne bruger nu en række vektorer og en stadig mere avanceret vifte af værktøjer og teknikker: De stjæler legitimationsoplysninger, installerer malware, der sletter sig selv for at undgå afsløring, ændrer interne processer og omdirigerer netværksdata, benytter Social Engineering-svindel og angriber endda medarbejdernes mobiltelefoner og hjemmeenheder.

Organisationer implementerer flere og flere sikkerhedsværktøjer som værn mod disse trusler. Da disse løsninger er beregnet til at løse specifikke problemer, kan de sjældent fungere sammen. Mange anvender særligt tilpassede dashboards, konsoller og logfiler. Problemer med integrationen gør det svært at få et samlet overblik og prioritere truslerne hurtigt. Det bliver en endnu større udfordring, når man arbejder med både cloud-ressourcer og on-premises-ressourcer. Som et resultat kan angreb foregå i over 140 dage uden at blive opdaget.[2]

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

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

Prøv dette

Da hurtig afsløring og respons bliver stadig vigtigere, kan disse bedste praksisser anbefales:

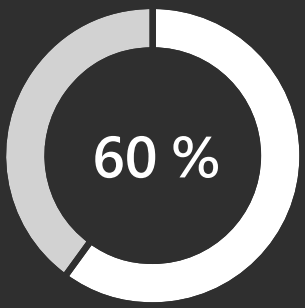
- Få et holistisk overblik over sikkerheden for hele netværket, herunder cloud-og hybridmiljøer.
- Opbyg et økosystem af sikkerhedsprodukter og-platforme, der er indbyrdes integrerede og leverer indsigtsdata.
- Samarbejd med teknologileverandører, der deler oplysninger på tværs af sikkerhedsbranchen.

Vigtige pointer

Manglen på integration mellem sikkerhedsprodukter gør det svært for sikkerhedsteams hurtigt at se og bekæmpe trusler i en koordineret og samlet løsning.

Vælg produkter, der er designet til at blive integreret med andre produkter.

2. Administrer adgang via identitet, ikke via endpoints



af alle sikkerhedsbrud stammer fra et kompromitteret endpoint.[3]

Et brud på datasikkerheden kan have enorme omkostninger. En måde at bekæmpe de høje omkostninger på er at etablere de fornødne sikkerhedskontroller til at opnå indblik i trusler og angreb. Men sikkerhedsteams er også nødt til at understøtte brugertilpassede it-løsninger, da medarbejderne ikke længere kun arbejder på stramt styrede enheder fra virksomheden, men forventer at kunne arbejde hvor som helst, på enhver enhed eller enhver platform, uanset om den er blevet godkendt af virksomhedens it-afdeling.

I virkelighedens verden knytter identitetsdrevne strategier adgangen til identiteter, ikke til enheder. Anvend kontrolfunktioner baseret på roller og behov, uanset hvordan brugeren har adgang. Denne tilgang fokuserer på godkendelse og administration af brugere, når de får adgang til virksomhedens aktiver, så organisationerne kan beskytte deres data, uanset hvor de er lagret, hvordan de tilgås, eller med hvem de deles.

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

Prøv dette

Det er en mere robust tilgang at skifte fra en sikkerhedsstrategi, der udelukkende handler om endpoints. Disse værktøjer kan hjælpe:

- Løsninger **til identitets- og adgangsstyring (IAM) og til administration af mobilapplikationer med** løsninger til forebyggelse af datatab (DLP). Begge reducerer risikoen ved at beskytte adgangen til applikationer og data i virksomhedens ressourcer og i skyen. IAM kan eliminere behovet for flere legitimationsoplysninger ved at give medarbejderne en enkelt identitet for at få adgang til ressourcer i skyen og on-premises. Cloudbaserede IAM-systemer kan også benytte viden om og analyser af trusler fra teknologiudbyderen for bedre at kunne registrere unormale loginforsøg og automatisk reagere hensigtsmæssigt.
- **Multifaktorgodkendelse (MFA)** tilbyder et andet beskyttelseslag, som kræver, at brugerne benytter noget, de kender (deres adgangskode), og noget, de har (sekundær godkendelse via en enhed, fingeraftryk eller ansigtsgenkendelse). Andre robuste taktikker omfatter adgang ud fra brugerrisiko, enhedsrisiko, applikationsrisiko og endda placeringsrisiko. Disse funktioner kan automatisk tillade, blokere eller kræve MFA af en bruger i realtid baseret på de politikker, du har fastsat, hvilket grundlæggende lader organisationerne øge beskyttelsen ved deres egen hovedindgang.

Vigtige pointer

En identitetsdrevet sikkerhedsstrategi flytter fokus fra at spore endpoints (enheder) til at administrere de brugere, der opnår adgang til virksomhedens data.

Mere robust beskyttelse af endpoints giver indsigt i forebyggende metoder efter et brud.

3. Indfør en nultillidsmodel til bekæmpelse af trusler

17.000
malwareadvarsler

Det er, hvad gennemsnitlig organisation skal nå at gennemgå hver uge.[4]

Hackere ved, at enhver organisation har flere indgangspunkter. De bruger phishing-svindel, malware og spyware-angreb, udnytter browsere og software, søger adgang gennem mistede og stjålne enheder, social engineering, og andre taktikker til at bryde din sikkerhed. Det kræver konstant årvågenhed at bevare et tilstrækkeligt overblik på tværs af de trusler, du allerede har registreret, og lægge mærke til nye sårbarheder.

Nogle værktøjer kan bidrage til den konstante opmærksomhed på sikkerheden, men en bredere tilgang giver mere mening. Traditionelle værktøjer fokuserer på forebyggelse, men dette er ikke længere tilstrækkeligt. Organisationer skal antage, at der enten allerede er sket et brud, eller at der snart vil opstå et. Dette kaldes nul-tillidsmodellen. Derefter skal de finde de metoder, de skal benytte for nedbringe den tid, der kræves for at opdage og genoprette efter bruddet, markant.

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

Prøv dette

Vær sikkerhedsekspert på avanceret niveau. Det kan være nødvendigt at kigge bagud, hvis man vil bevare sit forspring i forhold til truslerne – lære af tidligere sikkerhedsbrud og aktiviteter og trin, som hackerne foretog.

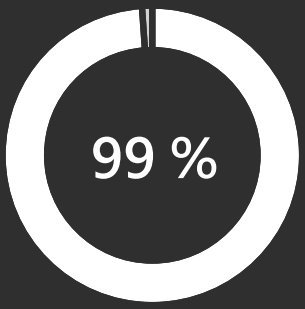
- Mange sikkerhedsapplikationer bruger indbyggede analyse- og maskinlæringsfunktioner til at analysere, hvordan en hacker har opnået adgang. Flere avancerede sikkerheds- og analyseløsninger vil benytte disse data til automatisk for at forhindre og håndtere lignende sikkerhedsbrud, hvilket er med til at reducere problemløsningstiden betragteligt.
- Den enorme bredde og dybde på det signal og den intelligens, der ligger bag disse løsninger, og kombinationen af erfaring og viden fra menneskelige eksperter, kan omdanne disse løsninger til effektive værktøjer mod truslernes konstante udvikling.

Vigtige pointer

Cloudbaserede applikationer kan lettere understøtter en nul-tillidsmodel, end ældre applikationer kan.

Ældre applikationer kræver modernisering for at understøtte identitetsbaseret betinget adgang.

4. Skift sikkert til skyen



af cloud-sikkerhedsnedbrud vil være kundens fejl til og med 2025.[5]

Hver organisation er på hver sit stadie af deres rejse til skyen. Krav om overholdelse af regler, lokale bestemmelser og andre overflytningsudfordringer betyder, at ikke alle organisationer er klar til at flytte vigtige arbejdsopgaver til skyen. Hybrid cloud-strategier er én tilgang, organisationer kan benytte som gradvis overgang til skyen, hvor de på samme tid bevarer nogle workloads on-premises og migrerer andre til skyen.

Cloud-servicemodeller påvirker, hvordan tjenesteudbydere og kunder fordeler ansvaret mellem sig. Dette rejser spørgsmål for CISO'er om, hvordan de skal håndtere udfordringerne ved at slippe nogle af kontrolfunktionerne i de on-premises-løsninger af hensyn til den overordnede sikkerhed, som cloud-leverandørerne kan tilbyde.

Tommelfingerreglen for sikkerheden i skyen er, at den er et fælles ansvar. Cloud-udbydere skal sørge for at have det sidste nye inden for sikkerhed og kryptering, mens kunderne blot skal sikre, at de tjenester, de køber, reelt er sikre, og at de nødvendige sikkerhedspolitikker også omfatter deres nye cloud-ressourcer.

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

Prøv dette

Stil de rigtige spørgsmål. Evaluering af cloud-udbydere handler ikke bare om at vælge en tjeneste. Det er et valg af, hvem du betror dine data til. Dette er nogle af de vigtige spørgsmål om sikkerhed og adgangskontrol, du skal stille:

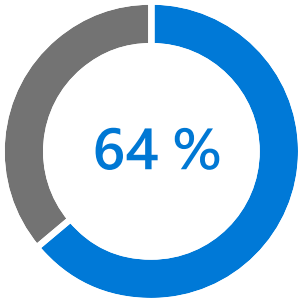
- Er vores data beskyttet af den sidste nye og supereffektive sikkerhedsteknologi?
- Implementerer I påkrævet beskyttelse af personlige oplysninger, og tillader I kontrol af vores data i vores virksomheds cloud-løsning?
- Hvordan har I investeret i robuste og innovative overholdelsesprocesser, som kan hjælpe os med at overholde gældende krav og bestemmelser?
- Hvor vil vores data blive opbevaret, hvem har adgang til dem, og hvorfor?
- Gennemfører I årlige tredjepartsevalueringer for at sikre, at sikkerheds-og overholdelsesstandarder bliver overholdt?
- Vil I afvise eventuelle anmodninger om videregivelse af kunders personlige oplysninger, der ikke er juridisk bindende?
- Overholder I standarderne for overholdelse og lovkrav i forskellige lande og områder, og i så fald hvilke?

Vigtige pointer

Når du skal evaluere udbydere af cloudtjenester, skal du sikre dig, at de overholder de internationale standarder.

Søg efter leverandører, der leverer detaljerede oplysninger om, hvordan deres tjenester fungerer, og hvordan de håndterer data.

5. Få et godt indblik i skygge-it



af medarbejdere har oprettet mindst én konto (med tilmelding til arbejdsrelateret website eller app) uden at involvere it-afdelingen.[6]

Når en medarbejder opretter en cloudbaseret konto uden en virksomheds tilladelse eller viden, kaldes det skygge-it. Kontoen virker ganske harmløst: Det kan f.eks. værktøj til grammatikkontrol på skrift. Men disse konti medfører sårbarheder, selv i de stærkeste sikkerhedskonfigurationer.

Personer, der opretter en sådan konto, vil ofte acceptere vilkår og betingelser uden at læse dem, og uden fuldt ud at forstå, hvad de giver adgang til. Traditionelle netværkssikkerhedsløsninger er ikke designet til at beskytte data i SaaS-apps og kan ikke give it-personalet et overblik over, hvordan medarbejderne bruger skyen.

I sidste ende ønsker vi ikke at undertrykke de motiver, der ligger bag skygge-it. At give medarbejdere og teams mulighed for at bruge de cloudapplikationer, der passer bedst til deres arbejdsformer, er med til at øge produktiviteten og innovationen. Sikringen af synlighed, kontrol og trusselsbeskyttelse i skygge-SaaS-apps er de første skridt i håndteringen af risici og facilitering af den digitale transformation, der allerede er i gang i din virksomhed.

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

Prøv dette

Få de oplysninger, du skal bruge. CASB'er (Cloud Access Security Broker) giver organisationer et detaljeret billede af, hvordan deres medarbejdere benytter skyen:

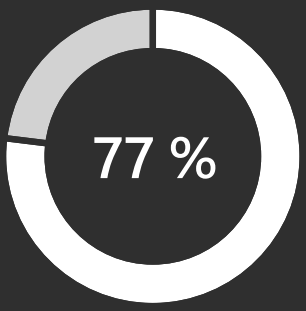
- Hvilke cloudapps bruger medarbejderne?
- Hvilken risiko udgør disse apps for organisationen?
- Hvordan får du adgang til disse applikationer?
- Hvilken slags data bliver der sendt til og delt fra disse applikationer?
- Hvordan ser upload/download-trafikken ud?
- Er der nogen uregelmæssigheder i brugeradfærden som f.eks. umulig transport, mislykkede logonforsøg eller mistænkelige IP-adresser?

Vigtige pointer

CASB'er (Cloud Access Security Broker) kan give dig et detaljeret billede af, hvordan medarbejderne bruger skyen.

Med bedre synlighed kan du angive politikker, der sporer og styrer, hvordan medarbejderne bruger disse apps.

6. Skab fuld integration mellem beskyttelse og produktivitet



af CISO'er siger, at de føler sig fanget mellem at lade folk arbejde frit og holde virksomheden beskyttet.[7]

Data bevæger sig nu uden for din kontrol oftere end nogensinde, da dine medarbejdere, partnere og kunder deler dem. Dette øger produktiviteten og fremme udviklingen, men det kan få betydelige konsekvenser, hvis meget følsomme data falder i de forkerte hænder. Sikkerhedscheferne skal administrere og sikre data, der er lagret flere steder og deles på tværs af internationale grænser i overensstemmelse med lovgivningen.

Medarbejderne kan kun magte det ekstra besvær til en vis grad, før de begynder at søge efter muligheder for at omgå sikkerhedskravene. Klassificering og kryptering er de bedste metoder til at beskytte data, mens brugen og delingen af oplysninger stadig er praktisk og effektiv. Du kan undgå menneskelige fejl ved at automatisere dataklassificeringen. Værktøjer kan forstå konteksten af data, såsom kreditkortnumre i en fil, eller følsomheden af data baseret på dataenes oprindelse. Efter afmærkningen kan visuelle markører som f.eks. sidehoveder, sidefødder og vandmærker samt beskyttelsesforanstaltninger såsom kryptering, godkendelse og brugsrettigheder automatisk anvendes på de følsomme data.

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

Prøv dette

Bliv fortrolig med detaljerne. Sikkerhedsteams bør altid kunne spore aktiviteter i forbindelse med meget fortrolige eller forretningsmæssigt vigtige filer og tilbagekalde adgangen til dem, hvis det er nødvendigt.

- Dette konstante beskyttelsesniveau følger dataene og beskytter dem hele tiden – uanset hvor de opbevares, eller med hvem, de bliver delt.
- Et identitetsstyringssystem letter arbejdet med at spore særligt fortrolige filer.

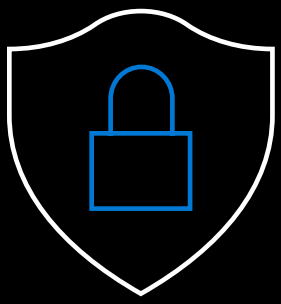
Vigtige pointer

Sikkerhed på dataniveau er alles ansvar.

Klassificering og mærkning af data skal ske på oprettelsestidspunktet, og sikkerhedsteams skal kunne overvåge aktiviteter i forbindelse med filerne, så de hurtigt kan skride til handling.

Microsoft

Konklusion



Cybertruslernes mangesidede karakter betyder, at det ikke længere er tilstrækkeligt at løse blot nogle af dine sikkerhedsmæssige udfordringer. Alle virksomhedens sikkerhedsbehov er unikke, men virksomhederne står over for de samme udfordringer og bærer samme ansvarsbyrde for at beskytte data, mennesker og systemer, mens innovationen og væksten ikke bliver forstyrret. Du har brug for fleksible sikkerhedsstrukturer, der fremmer og støtter den digitale transformation, understøttet af integrerede holistiske sikkerhedsstrategier for teknologier, processer og uddannelsesprogrammer.

Hvis du ikke har overvejet at migrere til skyen, er dette et godt tidspunkt at undersøge de mange nye sikkerhedsfunktioner, cloud-løsninger kan tilbyde. Microsoft 365 tilbyder en komplet, intelligent løsning til virksomheder af alle størrelser, som understøtter din digitale transformation med sikkerheds- og overholdelsesfunktioner, der er indbygget på alle niveauer.

Få mere at vide i denne tilbundsgående webinarserie uden omkostninger.

Se serien >