Microsoft

Sex steg mot en heltäckande säkerhetsstrategi

Den här informationen är avsedd för dig

som är IT-säkerhetsdirektör eller IT-säkerhetschef och:

- Vill få en snabb och tydlig guide till en övergripande säkerhetsstrategi.
- Vill hålla dig informerad om de senaste säkerhetsteknikerna.

Beräknad lästid: under 9 minuter

Innehåll

Ta itu med utmaningen 4

1. Använd integrerade säkerhetsprodukter för att möjliggöra snabba motåtgärder 5
2. Hantera åtkomst via identiteter – inte slutpunkter 7
3. Använd en noll förtroende-modell för att besegra hot 9
4. Flytta till molnet på ett säkert sätt 11
5. Få en helhetsbild av skugg-IT 13
6. Integrera skyddet i produktiviteten 15

Slutsats 17

Ta itu med utmaningen

Skyddet av data och system har högsta prioritet för alla organisationer. Den här utmaningen blir dock hela tiden svårare att hantera i takt med att angreppen blir allt mer avancerade, medarbetarna använder allt fler typer av enheter och program och data flödar in i och ut ur ditt företag på fler sätt. Massomställningen till distansarbete gör dessutom säkerheten ännu mer utsatt.

Ledarna måste balansera dessa utmaningar mot behovet av att samarbeta, förnya och utveckla ett företag. Du behöver en mångfacetterad säkerhetsmetod som ständigt skyddar alla slutpunkter, upptäcker tidiga tecken på ett intrång och reagerar innan skador hinner uppstå. Oavsett hur starkt ditt försvar är räcker det inte längre med förebyggande åtgärder. Du måste även anta en strategi med beredskap för intrång som innehåller funktioner för identifiering och motåtgärder.

Dagens IT-säkerhetsdirektörer behöver smidiga säkerhetsramverk som möjliggör digital omvandling och stöds av helhetsstrategier inbäddade i teknik, processer och utbildningsprogram. Även om allt detta är tillgängligt för lokala lösningar, är sanningen att en flytt till molnet omedelbart förbättrar säkerhetsfunktionerna i hela organisationen.

> **Den här e-boken innehåller IT-säkerhetsdirektörernas sex bästa strategier för att göra säkerheten till en hörnsten i företagets framgång. Dessa strategier är avsedda för ett lokalt scenario, men är oändligt mycket enklare att uppnå i ett molnscenario.**

1. Använd integrerade säkerhetsprodukter för att möjliggöra snabba motåtgärder

75

Antal säkerhetsprodukter som en genomsnittlig stor organisation använder.[1]

Angriparna har utvecklat sina verksamheter från smash-and-grab-angrepp för att ta sig in i system och kunna upprätthålla en beständig och långsiktig närvaro. De utnyttjar nu i stället en mängd olika angreppssätt och alltmer avancerade verktyg och tekniker: de stjäl autentiseringsuppgifter, installerar skadlig kod som raderar sig själv för att undvika upptäckt, ändrar interna processer och dirigerar om nätverksdata, använder social manipulation och angriper även medarbetarnas mobiltelefoner och privata utrustning i deras hem.

Organisationerna distribuerar allt fler säkerhetsverktyg för att skydda sig mot dessa hot. Dessa lösningar är oftast avsedda att hantera specifika problem och kan sällan användas tillsammans. Många använder egenutvecklade instrumentpaneler, konsoler och loggar. De bristande integrationsmöjligheterna gör det svårt att få en övergripande vy och snabbt prioritera hanteringen av hot. Utmaningen blir ännu större för de företag som använder sig av både molnbaserade och lokala resurser. Det innebär att angrepp kan förbli oupptäckta i över 140 dagar.[2]

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

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

Prova detta

Följande bästa praxis har utkristalliserats i takt med att snabb detektering och snabba motåtgärder har blivit allt viktigare:

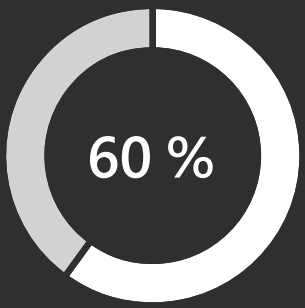
- Skapa en helhetsbild av säkerheten för hela nätverket, inklusive moln- och hybridmiljöer.
- Bygg ett ekosystem av säkerhetsprodukter och -plattformar som integreras med varandra och ger insikter i säkerheten.
- Bli partner med teknikleverantörer som samarbetar och delar information med hela säkerhetsbranschen.

Viktiga insikter

Bristen på integration mellan olika säkerhetsprodukter gör det svårt för säkerhetsteamen att snabbt kunna identifiera och bekämpa olika hot.

Sök efter produkter som kan integreras med andra produkter.

2. Hantera åtkomst via identiteter – inte slutpunkter



av alla intrång sker via en utsatt slutpunkt.[3]

Ett dataintrång kan orsaka enorma kostnader. Att införa nödvändiga säkerhetskontroller som ger insyn i hot och angrepp är ett sätt att motverka att dessa höga kostnader uppstår. Men säkerhetsteamen måste även kunna stödja en konsumentcentrerad IT-miljö där medarbetarna inte längre bara arbetar via företagets hårt kontrollerade enheter, utan även förväntar sig att kunna arbeta var de än befinner sig och på valfri enhet eller plattform, oberoende av om företagets IT-avdelning har godkänt den aktuella lösningen.

De nya arbetssätten kräver därför identitetsdrivna säkerhetsstrategier som knyter åtkomsten till identiteter, inte till enheter. Tillämpa kontroller baserade på roller och behov – oavsett hur användaren ansluter. Autentiseringen och hanteringen av användarna när de ansluter till företagets resurser gör det även möjligt för organisationer att skydda sina data var dessa än lagras, hur de än används eller vilka de än delas med.

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

Prova detta

Växlingen från en säkerhetsstrategi som endast handlar om slutpunkter skapar en mer robust lösning. Följande verktyg kan hjälpa dig:

- **Lösningar för identitets- och åtkomsthantering (IAM)** och **hantering av mobilappar med dataförlustskydd (DLP)**. Båda bidrar till att minska risken genom att skydda åtkomsten till program och data i företagsresurser och i molnet. IAM hjälper medarbetarna att slippa hantera olika inloggningsuppgifter genom att ge dem en enda identitet som ger åtkomst till både molnbaserade och lokala resurser. Molnbaserade IAM-system kan även använda hotinformation och hotanalys från teknikleverantören för att enklare kunna identifiera onormala inloggningsförsök och automatiskt vidta lämpliga motåtgärder.
- **Multifaktorautentisering (MFA)** är ytterligare ett skyddslager som kräver att användarna kan visa upp något de känner till (sitt lösenord) och något de har (sekundär autentisering via en enhet, ett fingeravtryck eller ansiktsigenkänning). Andra kraftfulla metoder kan vara att basera åtkomst på användarrisk, enhetsrisk, programrisk eller platsrisk. De här funktionerna gör det möjligt att automatiskt tillåta, neka eller kräva MFA från en användare i realtid baserat på de policyer du anger – och gör det möjligt att öka säkerheten redan vid organisationens ytterdörr.

Viktiga insikter

En identitetsdriven säkerhetsstrategi flyttar fokus från att hålla ordning på ett växande antal slutpunkter (enheter) till att hantera vem som använder företagets data.

Det mer robusta slutpunktsskyddet ger även insikter i angriparens teknik efter ett eventuellt intrång.

3. Använd en noll förtroende-modell för att besegra hot

17 000

varningar om skadlig kod

Det genomsnittliga antal varningar som stora organisationer måste granska varje vecka.[4]

Hackare vet att varje organisation har flera ingångspunkter. De använder nätfiske, skadlig programvara och spionprogram, säkerhetsluckor i webbläsare och programvara, borttappade och stulna enheter, sociala bedrägerier och andra taktiker för att ta sig igenom din säkerhet. Du måste hela tiden vara vaksam för att behålla överblicken över de hot du redan känner till, samtidigt som du måste ha koll på framväxande sårbarheter.

Vissa verktyg kan hjälpa dig skapa en kontinuerlig säkerhet, men det kan ibland vara bättre med ett bredare angreppssätt. I traditionella verktyg ligger fokus på förebyggande funktioner, men det räcker inte längre idag. Organisationer måste utgå från att ett intrång antingen redan har inträffat eller att ett sådant kommer att inträffa inom kort. Detta kallas noll förtroende. Organisationerna måste sedan hitta lösningar som kraftigt minskar den tid som krävs för att identifiera och återhämta sig från intrånget.

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

Prova detta

Bli expert på avancerad säkerhet. Att ligga steget före hoten ger dig möjlighet att blicka tillbaka – att lära dig av tidigare incidenter, hackarnas aktiviteter och steg.

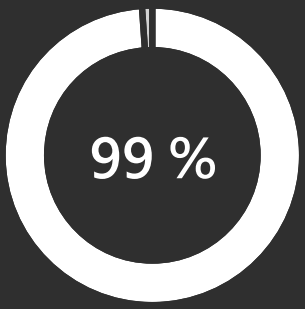
- Många säkerhetsappar har inbyggda analys- och maskininlärningsfunktioner som analyserar hur hackare lyckats få åtkomst till systemet. De mer avancerade säkerhets- och analyslösningarna använder sig av dessa insikter och agerar automatiskt för att förebygga och reagera på liknande intrång, vilket minskar tiden till skademinimering avsevärt.
- Bakom de här lösningarna finns en enorm mängd signaler och information, och i kombination med erfarenheten och kompetensen hos mänskliga experter kan de här lösningarna utgöra kraftfulla verktyg även mot snabba hotaktörer.

Viktiga insikter

Molnbaserade program har ett mer omfattande stöd för en noll förtroende-modell jämfört med äldre program.

De äldre programmen måste moderniseras för att stödja identitetsbaserad villkorsstyrd åtkomst.

4. Flytta till molnet på ett säkert sätt



av molnsäkerhetsbristerna kommer att vara kundens fel till 2025.[5]

Varje organisation gör sin egen resa till molnet. Kraven på regelefterlevnad, lokala föreskrifter och andra utmaningar i samband med migreringen innebär att alla organisationer inte är redo att flytta kritiska laster till molnet. Strategier för hybridmoln är ett sätt för organisationer att underlätta flytten till molnet genom att behålla vissa laster lokalt och flytta andra till molnet.

Molntjänstmodeller påverkar hur tjänstleverantörer och kunder fördelar ansvaret sinsemellan. Det här innebär att IT-säkerhetsdirektörerna måste ta ställning i ett antal frågor när det gäller att ge upp en del av kontrollen i de lokala lösningarna för att kunna ta del av den mer kraftfulla säkerheten hos en molnleverantör.

Tumregeln när det gäller säkerhet i molnet är ett delat ansvar. Molnleverantörerna måste ha en förstklassig säkerhet och kryptering, men kunderna måste se till att de tjänster som köps in faktiskt är säkra och att de säkerhetspolicyer som krävs även utvidgas till de nya molnresurserna.

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

Prova detta

Ställ de rätta frågorna. Utvärderingen av olika molnleverantörer handlar inte bara om att välja en tjänst, utan om vem du anförtror dina data. Här är några viktiga frågor du bör ställa angående säkerhet och åtkomstkontroll:

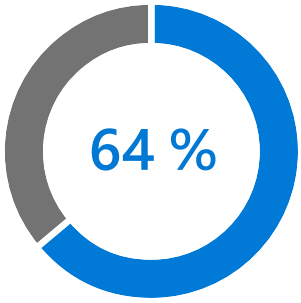
- Skyddas våra data med stark säkerhet och förstklassig teknik?
- Använder ni inbyggt dataskydd och tillåter kontroll över våra data i vårt företagsmoln?
- Vilka investeringar har gjorts i robusta och innovativa efterlevnadsprocesser som hjälper oss uppfylla våra efterlevnadskrav?
- Var kommer mina data att lagras, vilka har tillgång till dem och varför?
- Genomför ni årliga tredjepartsgranskningar för att säkerställa att säkerhets- och efterlevnadsstandarderna uppfylls?
- Kommer ni att avvisa eventuella begäranden om utlämnande av kundernas personuppgifter som inte är juridiskt bindande?
- Följer ni efterlevnadsstandarderna och regelverken i olika länder och på olika platser, och i så fall vilka?

Viktiga insikter

När du utvärderar olika leverantörer av molntjänster bör du försäkra dig om att de följer internationella standarder.

Sök efter leverantörer som publicerar detaljerad information om hur de driver sina tjänster och hanterar data.

5. Få en helhetsbild av skugg-IT



av medarbetarna har skapat minst ett konto (registrerat sig för en arbetsrelaterad webbplats eller app) utan att involvera IT-avdelningen.[6]

När en medarbetare skapar ett molnbaserat konto utan arbetsgivarens godkännande eller vetskap kallas detta för skugg-IT. Dessa konton kan verka helt ofarliga och kan till exempel utgöras av ett verktyg för att kontrollera grammatik. Men dessa konton skapar dock sårbarheter även vid användning av de mest omfattande säkerhetskonfigurationerna.

Människor accepterar ofta villkor utan att läsa igenom dem och utan att helt förstå vad de beviljar åtkomst till. Traditionella säkerhetslösningar för nätverk är inte utformade för att skydda data i SaaS-appar och ger inte IT-avdelningen insyn i hur medarbetarna använder molnet.

Vi vill inte dämpa den motivation som ger upphov till skugg-IT. När du låter dina medarbetare och team använda de molnprogram som passar deras arbete bäst ökar produktiviteten och innovationen främjas. Det första steget när det gäller att hantera riskerna och underlätta den digitala omvandling som redan pågår vid ditt företag är att få insyn i, kontroll av och skydd mot hot i SaaS-skuggappar.

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

Prova detta

Få den information du behöver. Säkerhetsförmedlingar för molnåtkomst (CASB:er) kan ge organisationer en detaljerad bild av hur medarbetarna använder molnet:

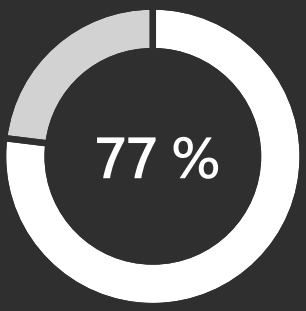
- Vilka molnappar använder medarbetarna?
- Vilka risker innebär de här apparna för organisationen?
- Hur kommer medarbetarna åt de här apparna?
- Vilken typ av data skickas till och delas från dessa appar?
- Hur ser trafiken ut avseende upp-/nedladdning?
- Förekommer det avvikelser i användarnas beteende, till exempel i form av omöjliga förflyttningar, misslyckade inloggningsförsök eller suspekta IP-adresser?

Viktiga insikter

Säkerhetsförmedlingar för molnåtkomst (CASB:er) kan ge dig en detaljerad bild av hur medarbetarna använder molnet.

En bättre insyn hjälper dig att konfigurera policyer som spårar och styr hur medarbetarna använder de här apparna.

6. Integrera skyddet i produktiviteten



av IT-säkerhetsdirektörerna säger att de känner sig fångade mellan att låta människor arbeta fritt och hålla företaget säkert.[7]

Data hamnar i allt större utsträckning utanför din kontroll när de delas mellan medarbetarna, partnerföretag och kunder. Det här ökar produktiviteten och främjar innovation, men om känsliga data hamnar i orätta händer kan det få stora konsekvenser. Säkerhetschefer måste hantera och skydda data som lagras på olika platser och delas över internationella gränser, enligt tillämpliga regelverk.

Medarbetarna tolererar bara en viss mängd praktiska hinder innan de börjar söka efter möjligheter att ta sig runt säkerhetskraven. Klassificering och kryptering är de bästa sätten att skydda dina data samtidigt som informationen kan användas och delas på produktiva sätt. Du kan komma runt den mänskliga faktorn genom att automatisera dataklassificeringen. Verktyg kan lära sig förstå sammanhang för data, till exempel kreditkortsnummer i en fil, eller hur känsliga data är baserat på varifrån de kommer. När dina data har märkts upp kan du automatiskt använda visuella markörer som sidhuvuden, sidfötter och vattenmärken, samt skydd som kryptering, autentisering och åtkomsträttigheter för känsliga data.

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

Prova detta

Känn dig bekväm med detaljerna. Säkerhetsteam bör även kunna spåra aktiviteten för strikt konfidentiella filer eller affärshemligheter och vid behov neka åtkomst.

- Det här heltäckande skyddet följer dina data och skyddar dem kontinuerligt, var de än lagras eller vem de än delas med.
- Ett identitets- och åtkomsthanteringssystem minskar bördan av att spåra strikt konfidentiella filer.

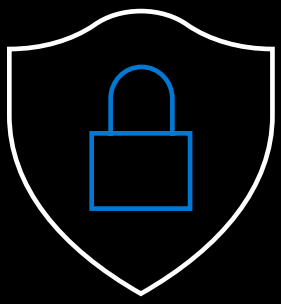
Viktiga insikter

Säkerhet på datanivå är allas ansvar.

Klassificering och uppmärkning måste ske i det ögonblick dina data skapas. Säkerhetsteam bör dessutom kunna övervaka filaktiviteter och vidta snabba åtgärder.

Microsoft

Slutsats



De många olika typerna av cyberhot innebär att det inte längre räcker med att bara lösa några av dina säkerhetsutmaningar. Varje företag har ett unikt säkerhetsbehov, men utmaningarna är ofta desamma och företagen måste skydda sina data, medarbetare och system samtidigt som innovation och tillväxt behöver främjas. Du behöver flexibla säkerhetsramverk som främjar och stöder digital omvandling och som understöds av holistiska säkerhetsstrategier som integrerats i teknik, processer och utbildningsprogram.

Om du inte redan har övervägt en flytt till molnet har du nu ett utmärkt tillfälle att utforska de utökade säkerhetsfunktioner som finns där. Microsoft 365 är en komplett och intelligent lösning för företag av alla storlekar. Den underlättar din digitala omvandling och har funktioner för säkerhet och regelefterlevnad inbyggda på varje nivå.

Få mer information i den här kostnadsfria och uttömmande webbseminarieserien.

Titta på serien >