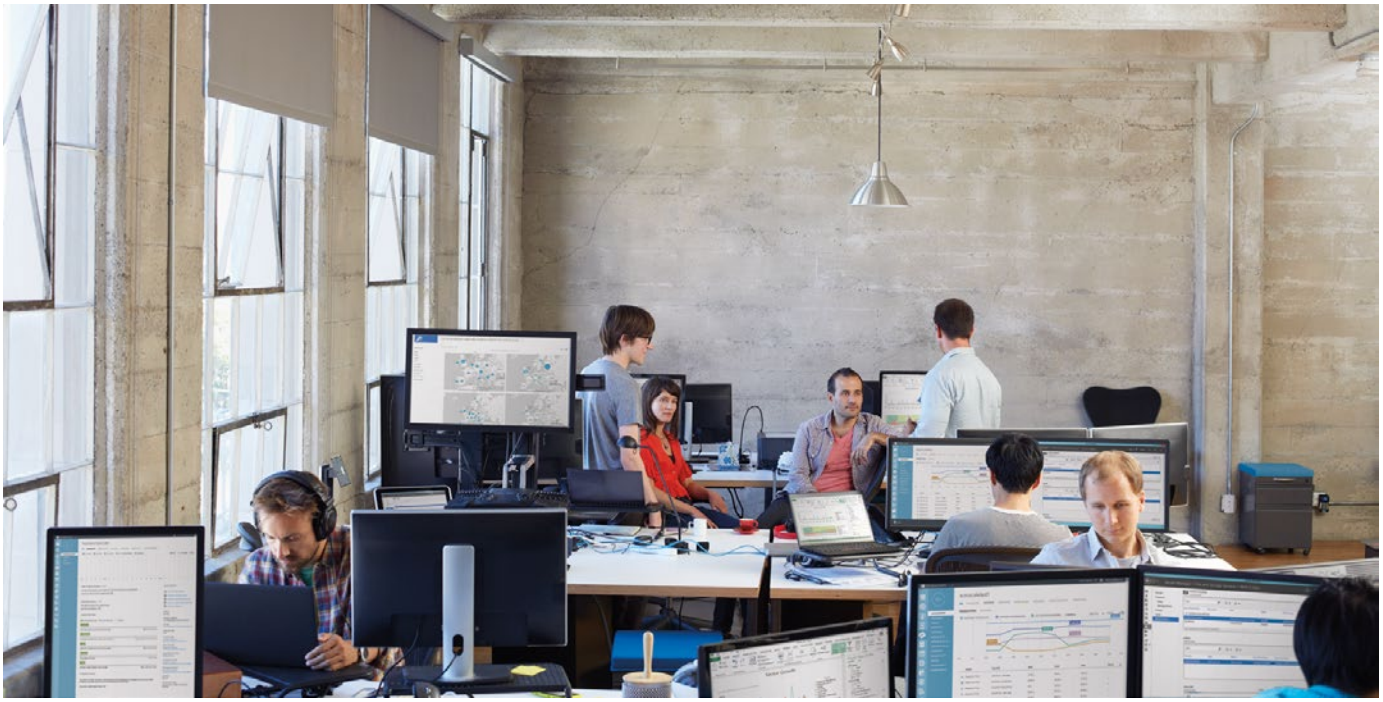
Microsoft

Hitta de svaga länkarna i verksamhetens säkerhetskedja



Förbättra ert skydd genom att snabbt hitta och övervaka säkerhetsproblem.

Med svaga länkar i säkerhetskedjans försvar, hur små de än är, blir företaget mottagligt för överträdelser som kan bli dyra. Den mest kostsamma effekten av cyberbrottslighet är just nu förlust av information, tätt följt av avbrott i verksamheten och förlorad produktivitet.[1] Kombinationen av dagens snabba företagsklimat och ett ökande behov av allt mer data och innovation skapar ett krav på att säkerheten utvecklas lika snabbt (eller snabbare) än hotbilden.

Effektiv säkerhet bygger på styrkan i hela kedjan – en enda svag länk kan påverka verksamheten märkbart. Här får du reda på vilka de vanligaste källorna till läckor är, vad de innebär för ditt företag och hur du skyddar hela nätverket bättre.

När säkerheten äventyras inifrån

Även med bästa möjliga säkerhetssystem kan en säkerhetskedja försvagas på grund av slutanvändarnas ofrivilliga misstag. Här följer en mer detaljerad undersökning av aktiviteter som kan leda till avbrott i säkerhetskedjan och tips på vad du kan göra för att undvika dem.

42 %

Även om hela 42 % av dataöverträdelser orsakas av tekniska fel är det ändå de mänskliga felen som står för den största andelen, med 58 %.[2]

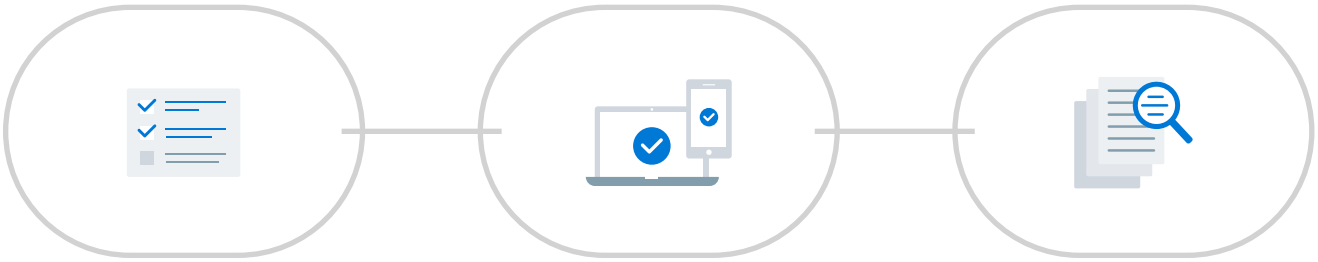
Möjliga överträdelser orsakade av interna eller externa medarbetare

Med det ökande antalet enheter och platser där medarbetare kan arbeta ökar även det potentiella hotet. Företag är inte längre bundna till en enda plats utan har numera verksamhet i olika länder och tidszoner, samtidigt som heltidsanställda, säljare och leverantörer är anslutna till system via flera enheter. För varje ny enhet och användare som är ansluten till nätverket finns även en ingångspunkt för en möjlig attack.

67 %

av IT-säkerhetsaktörer kan inte upptäcka vilka medarbetare som använder osäkra mobila enheter, som äventyrar känsliga data.[3]

Gör kedjan starkare:



01

När det är krångligt för medarbetare att komma åt information försöker de ofta hitta olika sätt att kringgå IT- och säkerhetsprinciper för att få jobbet gjort snabbt och effektivt. Se till att medarbetarna följer reglerna genom att ge dem enkel åtkomst till godkända företagsdata och verktyg på olika enheter, både på kontoret och på distans.

02

Dra nytta av hantering av multifaktorautentisering och mobilprogram för att förebygga obehörig åtkomst till företagsinformation.

03

Ge IT-avdelningen rätt verktyg för att övervaka och på distans kunna identifiera och lösa problem eller rensa enheter vid potentiella hot.

Interna avsiktliga överträdelser

Tyvärr händer det att anställda ibland avsiktligt missbrukar företagsdata. Även små läckor kan leda till omfattande förluster.

60 %
av medarbetare som lämnar sitt arbete med säkra data gör det i förhoppning om att dra nytta av den i framtiden.[3]

71 %
av fallen av internt missbruk handlar om personlig och medicinsk information.[3]

Gör kedjan starkare:

01
Använd verktyg som kan övervaka misstänkt aktivitet i nätverket och stänga ett användarkonto.

02
Anpassa åtkomst efter särskilda roller och ansvar inom organisationen.

03
Förenkla för IT-avdelningen att ge medarbetare åtkomst när de behöver den och ta bort den när det behovet inte längre finns.

Microsoft 365 E5

Ta reda på vilken Microsoft 365 Enterprise-lösning som passar ditt företag bäst

- Med avancerad säkerhetshantering för Office 365 får du översikt över misstänkt aktivitet så att du kan undersöka potentiella problem och vidta de säkerhetsåtgärder som behövs.
- Med Cloud App Security identifierar du alla molnappar i nätverket, får bättre översikt över skugg-IT och kan utvärdera risker – utan någon agent.
- Windows Hello för företag ersätter lösenord med stark tvåfaktorautentisering på datorer och mobila enheter. Det här är en ny typ av autentiseringsuppgifter som är knutna till en enhet och som använder biometrisk information eller PIN-kod.
- Azure Active Directory är en omfattande molnlösning för identitets- och åtkomsthantering som ger en stabil uppsättning funktioner för att hantera användare och grupper. Med den får du hjälp att säkra åtkomst till lokala program och program i molnet, bland annat Microsofts webbtjänster, som Office 365, samt många SaaS-program (programvara som en tjänst) som inte är från Microsoft.

När externa källor utgör ett hot mot infrastrukturen

En vanlig orsak till säkerhetsöverträdelser är attacker med avsikt att skada som är riktade mot organisationen utifrån. Metoder som exempelvis social manupilation har funnits så länge vi använt oss av e-post och surfat på Internet. Men med ökad medvetenhet har också angriparnas kreativitet ökat, så att även användare med gott omdöme riskerar att drabbas.[5]

3,3
miljarder autentiseringsuppgifter rapporterades stulna under 2016.[6]

23 %
av nätfiskeattacker via social manupilation lyckas, tack vare att mottagarna öppnar meddelandena.[6]

Här är fem vanliga typer av attacker via social manupilation:[7]

Nätfiske

Dirigerar om användare till misstänkta URL-adresser som verkar legitima, i syfte att stjäla autentiseringsuppgifter eller annan personlig information.

Pretexting

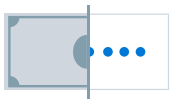
Skapar ett falskt scenario för att få användarens förtroende och på så sätt stjäla personlig information.

Baiting

Infekterade USB-minnen eller -diskar lämnas på allmänna platser i hopp om att någon tar den och sätter in den i en dator. Samma taktik används på webben i form av nedladdningsbara länkar.

Tailgating

Angripare får åtkomst till begränsade områden genom att följa efter en anställd som har korrekt autentisering.



Quid pro quo

Ger löfte om någon typ av förmån i utbyte mot information från offret.

Återställa data – till vilket pris

Utpressningstrojaner (data görs oåtkomliga tills du betalat en avgift) ökar inte bara i frekvens. Det är även så att fler drabbade betalar för att få tillbaka sina data. Undvik utpressningstrojaner genom att gå tillbaka till grunderna: medvetenhet, utbildning, gott omdöme, regelbunden säkerhetskopiering, en åtgärdsplan och, inte minst, programvara.

6 000 %

Från 2015 till 2016 ökade utpressningstrojaner med 6 000 %.[8]

40 %

Utpressningstrojaner fanns i nästan 40 % av alla skräppostmeddelanden under 2016.[8]

70 %

av de drabbade betalade hackarna för att få tillbaka sina data. Av dem som valde att betala, betalade 50 % mer än 100 000 kr och 20 % betalade mer än 400 000 kr.[8]

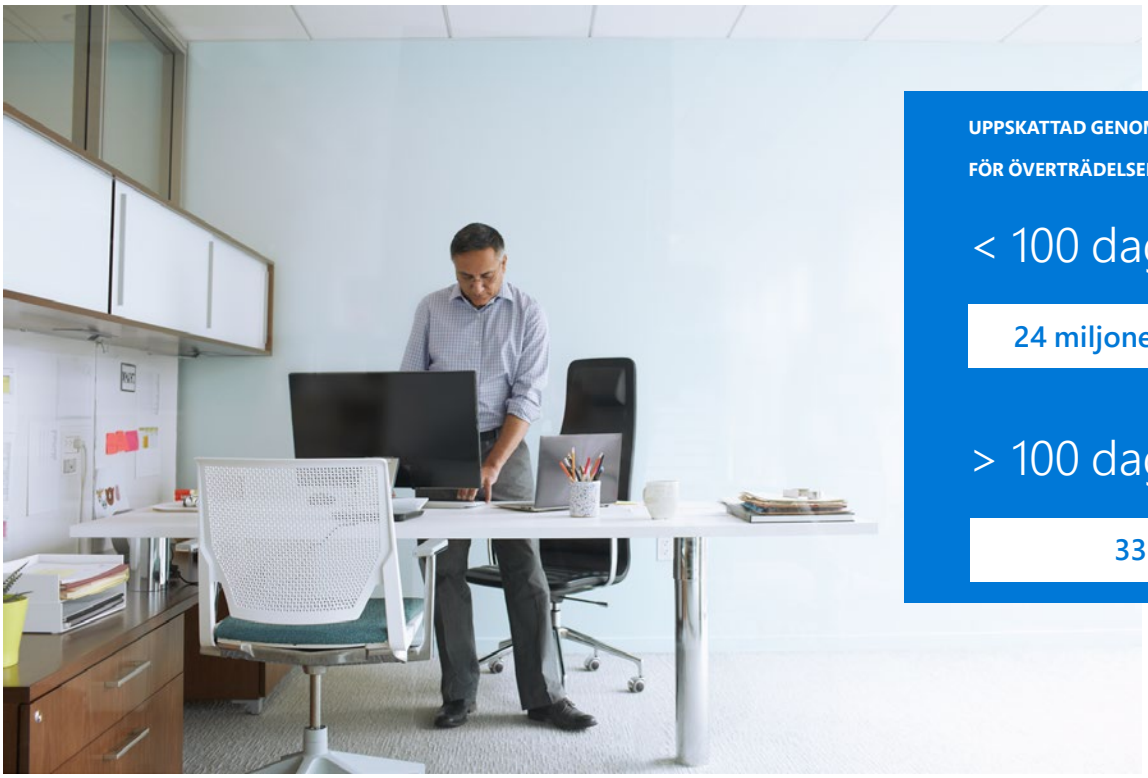
Microsoft 365 E5

Ta reda på vilken Microsoft 365 Enterprise-lösning som passar ditt företag bäst

- Med Windows Defender Antivirus i datorn skyddas system, filer och onlineaktiviteter mot virus, skadlig kod, spionprogram och andra slags hot.
- Office 365 Advanced Threat Protection skyddar företagets e-post i realtid mot både okända och sofistikerade attacker genom att säkra Office 365-miljön mot avancerade hot, osäkra filer och länkar till skadligt innehåll i sådana filer.
- BitLocker-diskkryptering fungerar smidigt med Windows 10 och inriktar sig på hot förknippade med datastöld eller exponering från borttappade, stulna eller felaktigt avställda datorer.

Identifiera och ta itu med säkerhetsöverträdelser snabbt

Kostnaden för en dataöverträdelse påverkas till stor del av den tid det tar att identifiera och få kontroll över den. Beroende på hur snabbt återställningen går kan du spara miljontals kronor.



UPPSKATTAD GENOMSNITTLIG KOSTNAD FÖR ÖVERTRÄDELSER[9]

< 100 dagar

24 miljoner kr

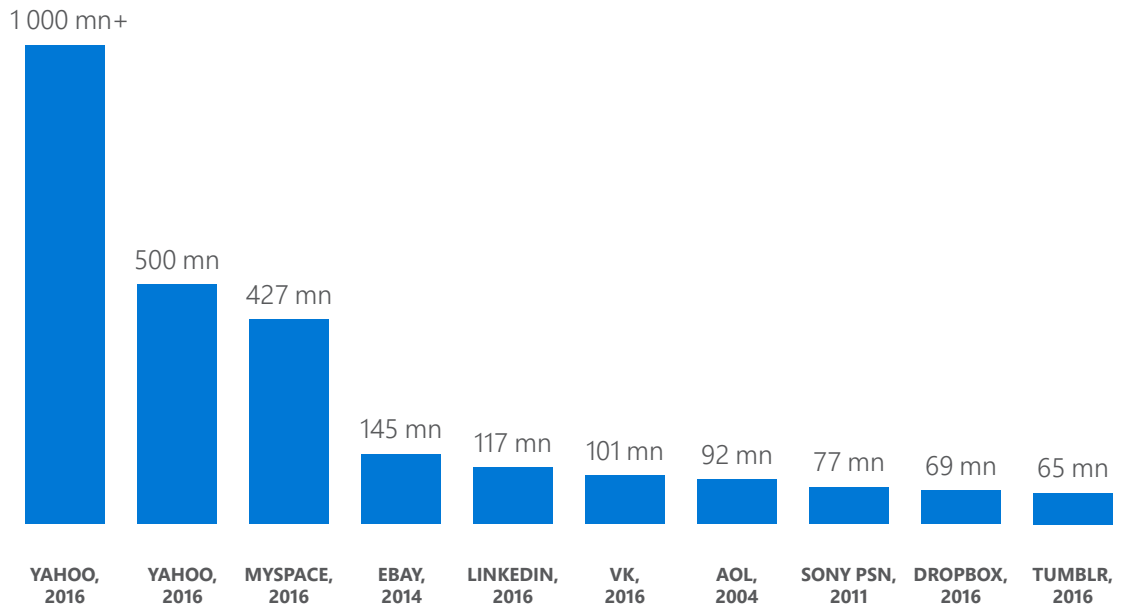
> 100 dagar

33 miljoner kr

Utan rätt verktyg för att snabbt upptäcka dataöverträdelser kan dessa bli kostsamma. Se nedan hur ett antal ledande företag drabbats av kostsamma överträdelser.

Om vi tänker på säkerheten som en kedja är det viktigt att varje länk i kedjan är tillräckligt stark. Att implementera snabba lösningar som visar sig otillräckliga kan få till följd att säkerheten äventyras, något du kanske inte inser förrän det är för sent.

Största dataöverträdelser, 2004–2016[10]



Globalt sett lyckades organisationer minska antalet dagar det tog att identifiera en dataöverträdelse från i genomsnitt 201 dagar 2016 till 99 dagar 2017. Det genomsnittliga antalet dagar för att få kontroll över en dataöverträdelse minskade från 70 till 66 dagar.[9] Ju snabbare en dataöverträdelse kan identifieras och kontrolleras, desto lägre blir kostnaderna. Det är därför viktigt att företag har de rätta verktygen för att snabbt kunna identifiera och få kontroll över dataöverträdelser.

Microsoft 365 E5

Ta reda på vilken Microsoft 365 Enterprise-lösning som passar ditt företag bäst

- Med Windows Defender Advanced Threat Protection kan du identifiera, undersöka och hantera avancerade attacker och dataöverträdelser i organisationenens nätverk.
- Med Advanced Threat Analytics minskar risken för kostsamma skador och du får tillgång till all nödvändig information i en tydlig realtidsvy som visar attackens tidslinje. All den information du behöver för att lära dig om, analysera och identifiera normala och misstänkta användar- och enhetsbeteende är dessutom inbyggd.
- Med Office 365 Threat Intelligence får du en bred insyn i hotbilden. Det som är viktigt att veta för dig visas och du får en fyllig översikt över hur de olika hoten kan påverka organisationen. Med den här typen av insyn och översikt kan organisationer uppdatera sina säkerhetspolicyer och tjänster för att undvika potentiella hot på ett förebyggande sätt.

Använd ett helhetsperspektiv för att ta itu med svaga länkar och göra hela säkerhetskedjan starkare.

Med Microsoft 365 får du fullt integrerade och heltäckande försvarsverktyg som hanterar alla delar i de åtgärder du vidtagit i säkerhetskedjan. Välj ett arbetssätt som är tillförlitligt, säkert och produktivt och som förser dig med den bästa säkerheten för din maskinvara, programvara och nätverk.

Upptäck hur Microsoft 365 Enterprise kan skydda din verksamhet med intelligenta lösningar som frigör kreativitet och gör att alla kan arbeta tillsammans på ett säkert sätt.

Källor:

1. "Cost of Cyber Crime Study & the Risk of Business Innovation", 2016, Ponemon Institute
2. "International Trends in Cybersecurity", 2016, Comptia
3. "The Cost of Insecure Mobile Devices in the Workplace", 2014, Ponemon Institute
4. "2017 Data Breach Investigations Report", 2017, Verizon
5. "2017 Credential Spill Report", Shape Security
6. "Anatomy of a Social Engineering Attack: Exploiting Human Behavior", 2016, PricewaterhouseCoopers
7. "5 Social Engineering Attacks to Watch Out For", 2015, The State of Security
8. "Ransomware: How Consumers and Businesses Value Their Data", 2016, IBM
9. "2017 Cost of Data Breach Study", Ponemon Institute
10. "Latest Yahoo Attack is the Largest Data Breach to Date", 2016, Statista