



Kostnaden för cyberbrottslighet och hur man skyddar information

INNEHÅLL



03 | Inledning

05 | Avslöjade myter om cybersäkerhet

13 | Hur brottslighet på internet påverkar företag

24 | Framtidens cybersäkerhet för företag

28 | Ordlista och fortsatt läsning

INLEDNING

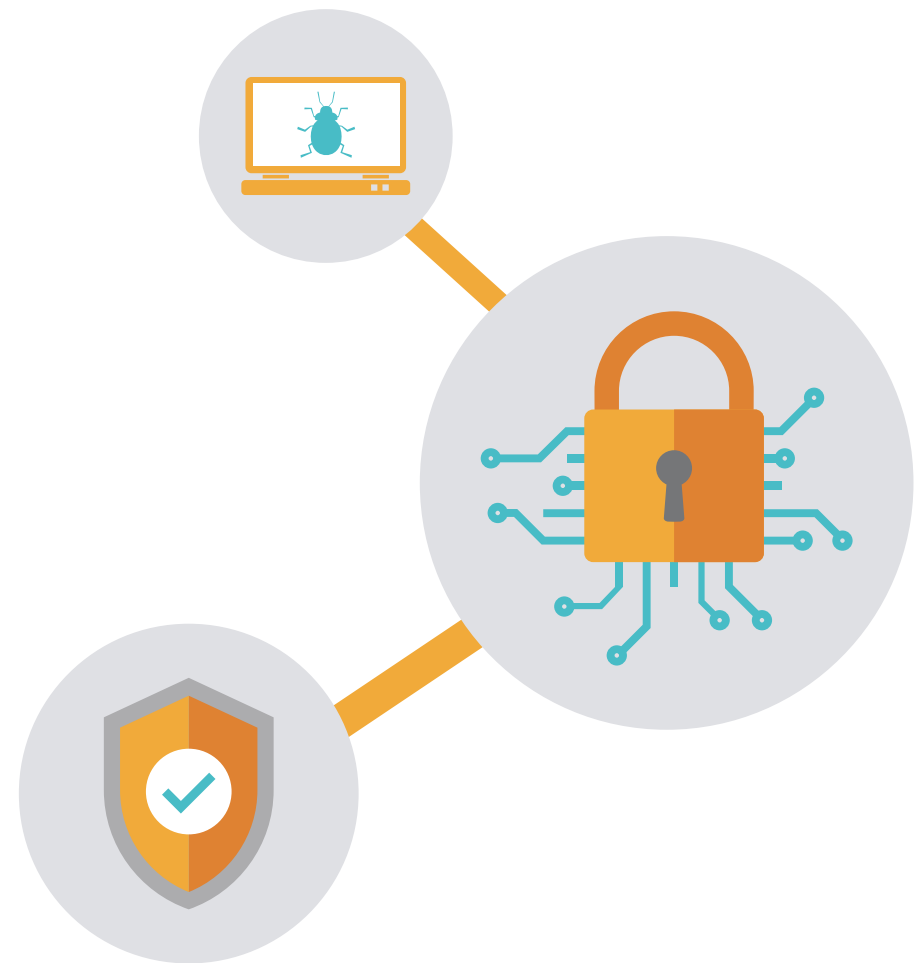
”Många företagsledare betraktar internet som den risk som är kännetecknande för vår generation.”
– Dennis Chesley, Global chef för riskbedömningstjänster, PwC¹

Cyberhot är inte ett nytt hot. Det är emellertid ett växande hot. Hackarna blir allt skickligare. De hittar fler och fler öppningar för att begå intrång i nätverk. ”Sakernas internet” multiplicerar antalet enheter och det är oftast den enklaste vägen att ta sig in. Mål som kan drabbas blir större och avbrott får större konsekvenser.

Den 21 oktober 2016 utsattes den USA-baserade DNS-leverantören Dyn för historiens mest omfattande DDoS-attack (Distributed denial of Service). Några av världens

största webbplatser – t.ex. Netflix,² Amazon och Twitter – stängdes ner i flera timmar.

Lloyds Bank utsattes under januari 2017 för betydande online-avbrott. Kunderna kunde inte kontrollera sina saldon eller utföra betalningar. Även tjänster via mobilappar var utslagna. Lloyds har inte bekräftat det, men orsaken misstänktes vara en DDoS-attack.³



INLEDNING



Brott som dessa betyder mer än dålig publicitet. De motsvarar betydande ekonomiska värden.

I Spiceworks undersökning om skrivarsäkerhet från 2016 säger 34 procent av organisationerna att intrång medförde en ökning av supportsamtal/supporttid, 29 procent att intrång reducerade produktiviteten/effektiviteten och 26 procent rapporterade ökade systemavbrott som ett problem.⁴

Nästan 60 procent av de säkerhetschefer som intervjuades för en IBM CSO-utvärdering sade att angriparnas sofistikerade överträffade deras organisations försvar.⁵ Det senaste decenniet har oroliga IT-chefer återopat

cybersäkerhet som ett av de tio största problemen, nu hamnar cybersäkerhet på andra plats i SIM Trends årliga undersökning.⁶

En stor del av dessa förluster kan förhindras. På följande sidor går vi igenom vanliga missuppfattningar om cybersäkerhet, hur cyberbrottsligheten påverkar verksamheter och vad du kan göra för att förstärka skyddet mot attacker. Avslutningsvis blickar vi in i framtiden och diskuterar vad som väntar och hur man förbereder sig.

FEM VANLIGA MISSUPPFATTNINGAR SOM KAN UTSÄTTA VERKSAMHETER FÖR RISKER FÖR CYBERBROTTLIGHET

Rubrikerna handlar ofta om dataintrång mot kändisar, men alla typer av organisationer är exponerade för riskerna. Här följer fem myter om cyberhot som kan utsätta företag för dataintrång.



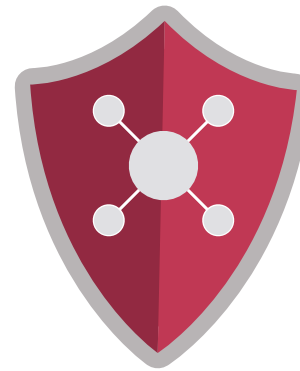
Säkerhets-
brott



Säkerhets-
luckor



Säkerhets-
rutiner



Antivirus-
program



Cyber-
attacker

1 FÖRETAG KAN SNABBT ÅTERHÄMTA SIG EFTER VARJE INTRÅNG



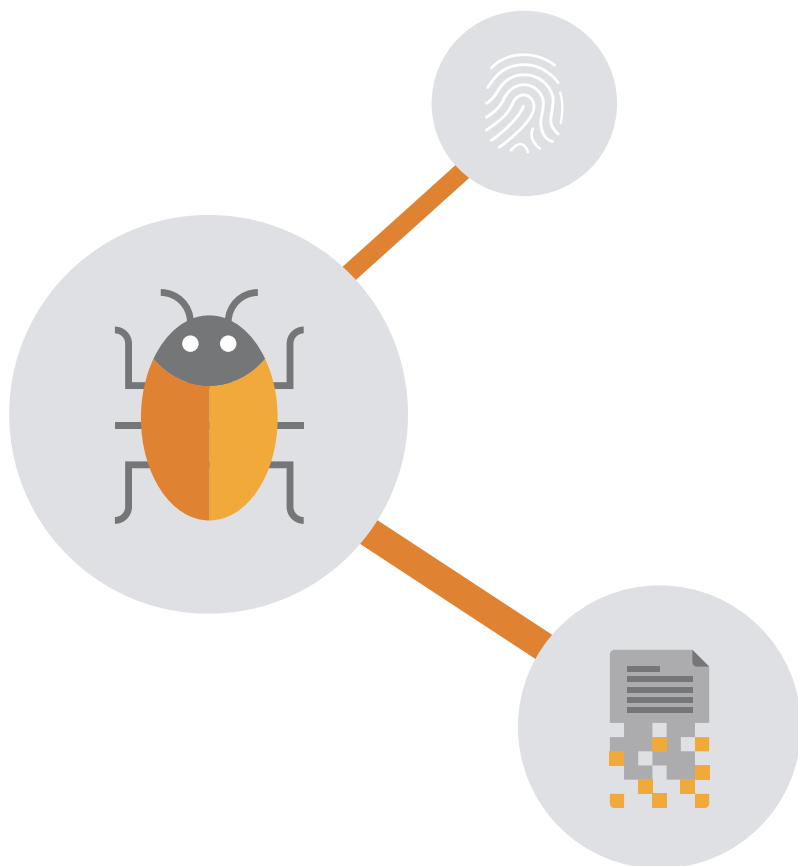
Det är fortfarande mycket svårt att mäta kostnaden för cybersäkerhetsöverträdelser mot kommersiella företag. Förr brukade man anta att man kunde se effekterna av eventuella brott genom sjunkande aktiekurser.

Aktiekursen är dock bara en del av historien – och en första del av vad det beträffar. Kurserna kan återhämta sig inom några veckor, men långsiktiga kostnader ackumuleras. Nya säkerhetsprogram. Ersättningspersonal. Juridikkostnader.

Alla dessa faktorer kan innebära betydande avbrott för verksamheter under lång tid efter ett dataintrång. Och kostnaderna ökar. En färsk Ponemon-studie visar att den genomsnittliga årliga kostnaden för ett dataintrång ökade från **61 miljoner kronor** år 2015 till **76 miljoner kronor** år 2016.⁷



2 SÄKERHETSLUCKOR ÄR SÄLLSYNTA, SÅ ETT OMFATTANDE SKYDD BEHÖVS INTE



IDC fann⁸ att andelen av företag som utsatts för dataintrång uppgick till 99 % under 2016. Samtidigt tog antalet företag som uppger sig ha utsatts för intrång 6–10 gånger under ett år ett skutt från 9 % 2014 till 18,9 % 2016.⁹

Dessa siffror kan mycket väl vara lågt värderade. Antalet rapporterade intrång är ofta underrapporterade när företagen försöker undvika åtföljande negativ publicitet.

Den andra punkten som denna myt förbiser är vilken försvagande effekt en säkerhetslucka kan ge. Ditt företag kanske bara drabbas en läcka. Men en läcka kan orsaka betydande utmaningar.

3 VI HAR ANLITAT EN IT-SPECIALIST FÖR ATT HANTERA SÄKERHETEN, SÅ VI HAR GJORT ALLT VI BEHÖVER



Att anlita en expert är en bra idé, men varje medarbetare i företaget bör också få utbildning i goda säkerhetsrutiner.

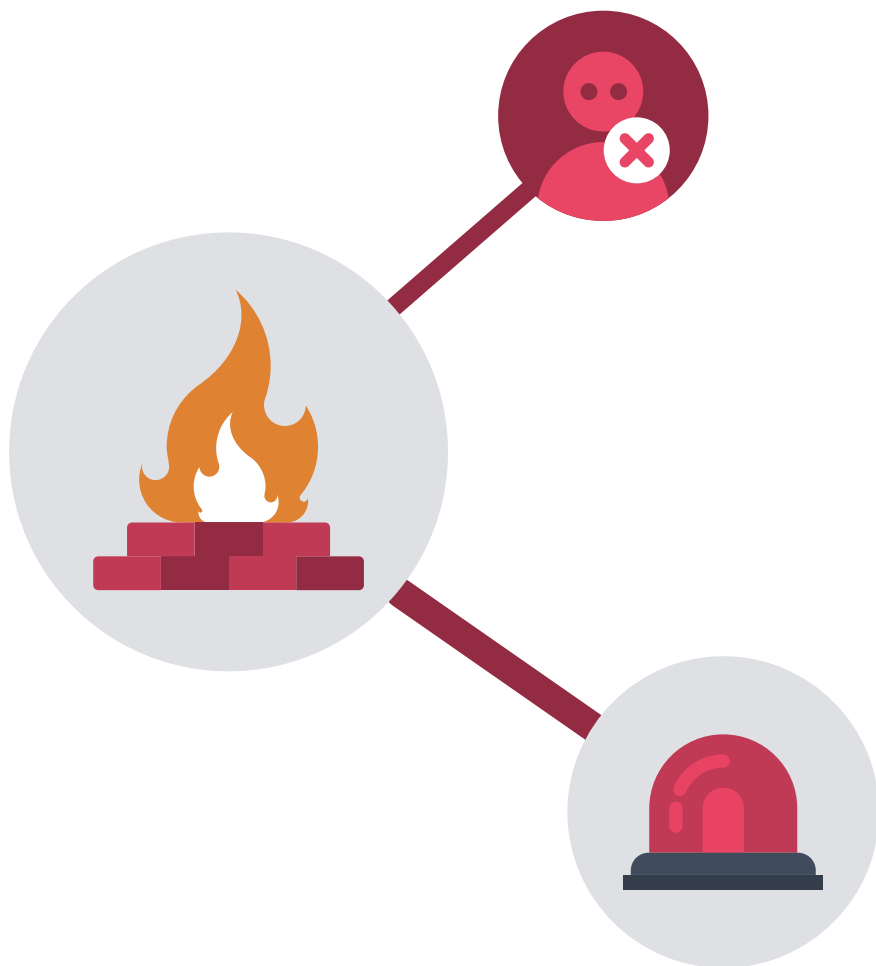
Tänk på medarbetaren som utan onda misstankar laddar ner ett e-postmeddelande med en bilaga som innehåller en skadlig kod eller besöker en osäker webbplats som infekterar företagets nätverk med skadlig programvara som gör datorer långsamma eller skickar känslig information till kriminella.

Enligt rapporten 2016 Cyber Threat från CyberEdge, rankade företag "låg medvetenhet om säkerhet bland anställda" som det största problemet för att företaget ska kunna skydda sig mot säkerhetshot. Detta problem rankades högre än "för liten budget" och "brist på kvalificerad personal".¹⁰



4

VI HAR BRA ANTIVIRUSPROGRAM I VÅRA SYSTEM OCH ÄR ALLTSÅ VÄL SKYDDADE



Antivirusprogram söker igenom system efter skadlig programvara som har laddats ner från webbplatser eller e-post. Hackarna har dock andra hjälpmedel för att kringgå detta skydd.

Dataintrång som inte kan blockeras av antivirusprogram är exempelvis DDoS-attacker (Distributed denial of Service), där en webbplats översvämmas med "skräptrafik" som gör att systemet arbetar långsammare eller slås ut; webbaserade attacker där hackare injicerar en skadlig kod på en webbplats för exempelvis datastöld, spionage eller för att skaffa åtkomst via stulna enheter.

5 OM EN INKRÄKTARE TAR SIG IN, UPPTÄCKER VI DET DIREKT



Det är inte enkelt att upptäcka en internetattack. Skadlig programvara som kommer in i ett system avbryter inte nödvändigtvis omedelbart dess funktion. Den kan spionera på systemet och ge inkräktaren information för mer riktade angrepp, ofta för att skaffa åtkomst i hela nätverket.

Sådana attacker på specifika system kategoriseras som APT-attacker (Advanced Persistent Threats). APT-attacker kännetecknas av kontinuerlig övervakning och inhämtning av data från speciella delar av infrastrukturen över tid – oftast utan att upptäckas.

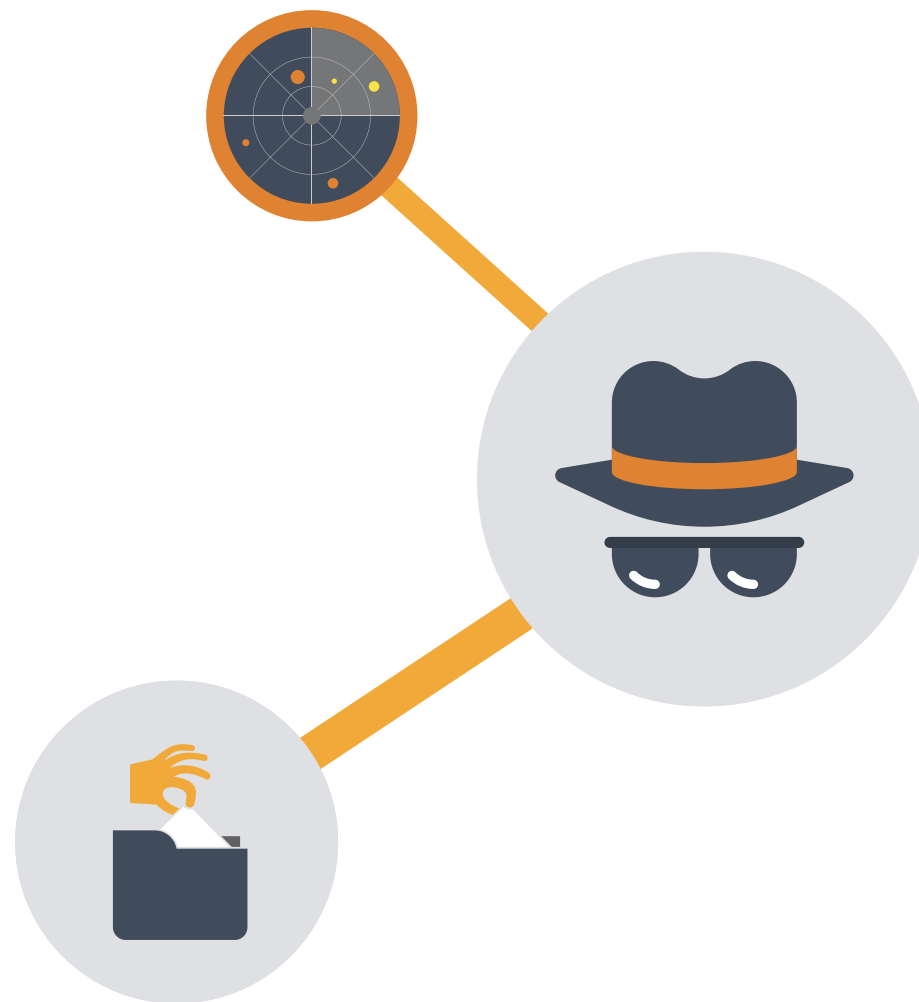
IT-konsultföretaget Daisy Group uppskattade att hälften av företagen i Storbritannien kan hackas på mindre än en timme.

TIPS:

Övervakning av utgående data avseende större flöde än vanligt kan bidra till att upptäcka datastöld – det kan vara en APT-attack.

AGERA:

Välj säkerhetsprogram med dataskydd, exempelvis HP SureStart som automatiskt återställer en dators BIOS när ett skadligt program upptäcks och stoppar intrång innan data har äventyrats.



VARIFRÅN KOMMER HOTEN?

Skyddet av nätverket börjar med medvetenhet om de svagaste länkarna

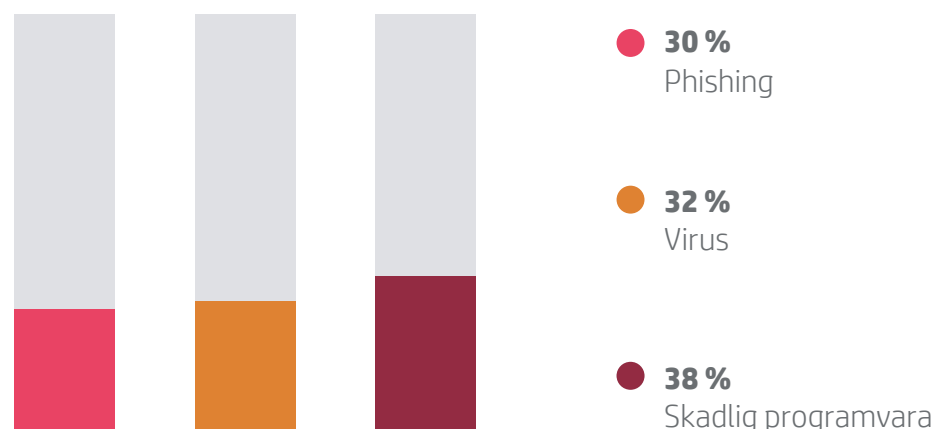
Den mest sannolika orsaken till dataintrång:¹¹



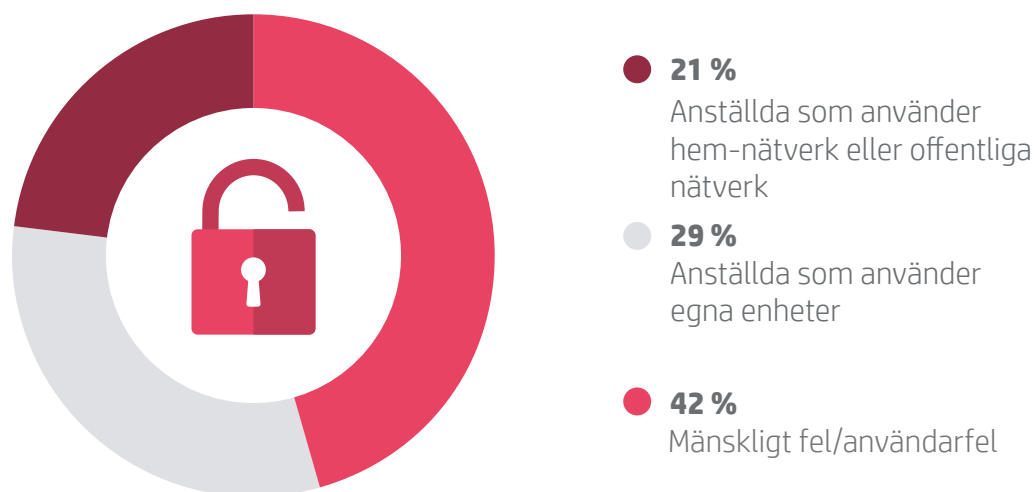
Externa hackare **1 = mest troligt 4 = minst troligt**



De vanligaste typerna av externa hot:



Hur interna intrång sker:¹²



HUR MYCKET KOSTAR ÅTERHÄMTNINGEN EFTER INTERNETBROTT?

Internetattackerna som kostar mest:

25 %

10 300 000 SEK

Skadliga koder och program

Programvara som skadar ett system genom att skapa säkerhetsluckor, förstöra filer eller stjäla data (t.ex. skript, virus och maskar)

24 %

9 900 000 SEK

Distributed Denial of Service

"DDoS"-attacker är flöden av webbttrafik som tar ner ett företags webbplats och servrar

16 %

6 600 000 SEK

Webbaserade attacker

Attacker riktade mot besökare på din webbplats, exempelvis injicerad kod som omdirigerar besökarna till platser med skadlig mjukvara

13 %

5 400 000 SEK

Stulna enheter

Anställdas förlorade enheter med åtkomst till inloggning på företaget kan orsaka datastöld och identitetsbedrägeri

9 %

3 700 000 SEK

Phishing (nätfiske) och social ingenjörskonst

E-post eller popup-fönster som ser ut som legitima förfrågningar om inloggningsuppgifter

9 %

3 700 000 SEK

Interna användare med onda avsikter

Anställda som skickar känsliga uppgifter

4 %

1 700 000 SEK

Botnät

Nätverk av infekterade datorer som har kontrollerats för skadliga aktiviteter, exempelvis att skicka skräppost

HUR BROTTSLIGHET PÅ INTERNET PÅVERKAR FÖRETAG

Den faktiska kostnaden för cyberbrottslighet gäller mer än att åtgärda skadorna som intrånget orsakat

Dataintrången kostar allt mer. Det finns generellt tre sätt som ett intrång kan drabba företagets ekonomi på.



Företagsresurser

Du måste självfallet ställa allt i ordning igen. För det krävs betydande insatser som tar anställdas tid. Du måste kanske låta annan intäktsskapande verksamhet vänta.



Avgifter eller böter

Du kan åläggas böter för brott mot efterlevnad (t.ex. HIPAA). När EU GDPR kommer nästa år kan företag man finner försumliga ådra sig böter på 4 % av sin totala omsättning. Du kan även utsättas för risker för rättegångar vid läckor som medför intrång i kunders konfidentiella information.



Skadat anseende

Detta kan vara en av de mest skadliga effekterna av ett intrång. Kunder, press och allmänheten har långt minne för brott mot säkerheten. Det kan ta lång tid att återupprätta förtroendet.

DET OVÄNTADE INTRÅNGETS ANATOMI

När Sony Pictures hackades under 2014, gick inkräktarna så att säga rakt in genom entrén.¹⁴

Enligt "Lena" i hackergruppen Guardians of Peace (GOP) – som tog på sig ansvaret för attacken – håller Sony "inte längre på med fysisk säkerhet". De skaffade åtkomst till Sonys nätverk genom att fysiskt gå in i byggnaden och stjäla systemadministratörens inloggningsuppgifter.

När de kommit in planterade de skadlig programvara som fångade privata filer, källkod och lösenord för Oracle- och SQL-databaser. Därefter stal de filmproduktionsplaner, e-post, ekonomidokument och annat – och publicerade mycket av detta online.

Inkräktarna hotade med att publicera flera hemliga och topphemliga uppgifter om företaget inte drog in filmen "The Interview" från biograferna.

Sony kapitulerade till slut, förlorade betydande biljettintäkter och ådrog sig väsentliga skador på sitt anseende.

Sony gjorde två misstag. Att inte prioritera fysiskt tillträde till företagets information av inkräktare och att inte investera i säkerhet med flera nivåer – vilket skulle ha kunnat hindra åtkomsten av känslig information efter det första intrånget.

Säkerhetsexperten Bruce Schneier skrev efter attacken: "Alla nätverk är sårbara mot en tillräckligt skicklig, ekonomiskt förmögen och motiverad angripare." Tricket är att känna till var nätverkets svaga punkter är. Det kan vara huvudentrén.

AGERA:

Skapa en åtgärdsplan för varje avdelning, från IT till kundtjänst, att följa för snabbare återhämtning efter intrånget.

TIPS:

Många typer av skadlig programvara sprids som e-postbilagor. Utbilda personalen i att känna igen misstänkta filer som ser ut att vara legitima dokument.

Databrottslighet: Återhämtningstiden

- Uppskattad kostnad för databrott mot företag i Storbritannien: 167 miljarder SEK¹⁵
- Genomsnittlig kostnad för databrott per företag i Storbritannien under 2016: 59 miljoner SEK¹⁶
- Företag i Storbritannien som under 2015–2016 utsattes för ett dataintrång: 66 %¹⁷

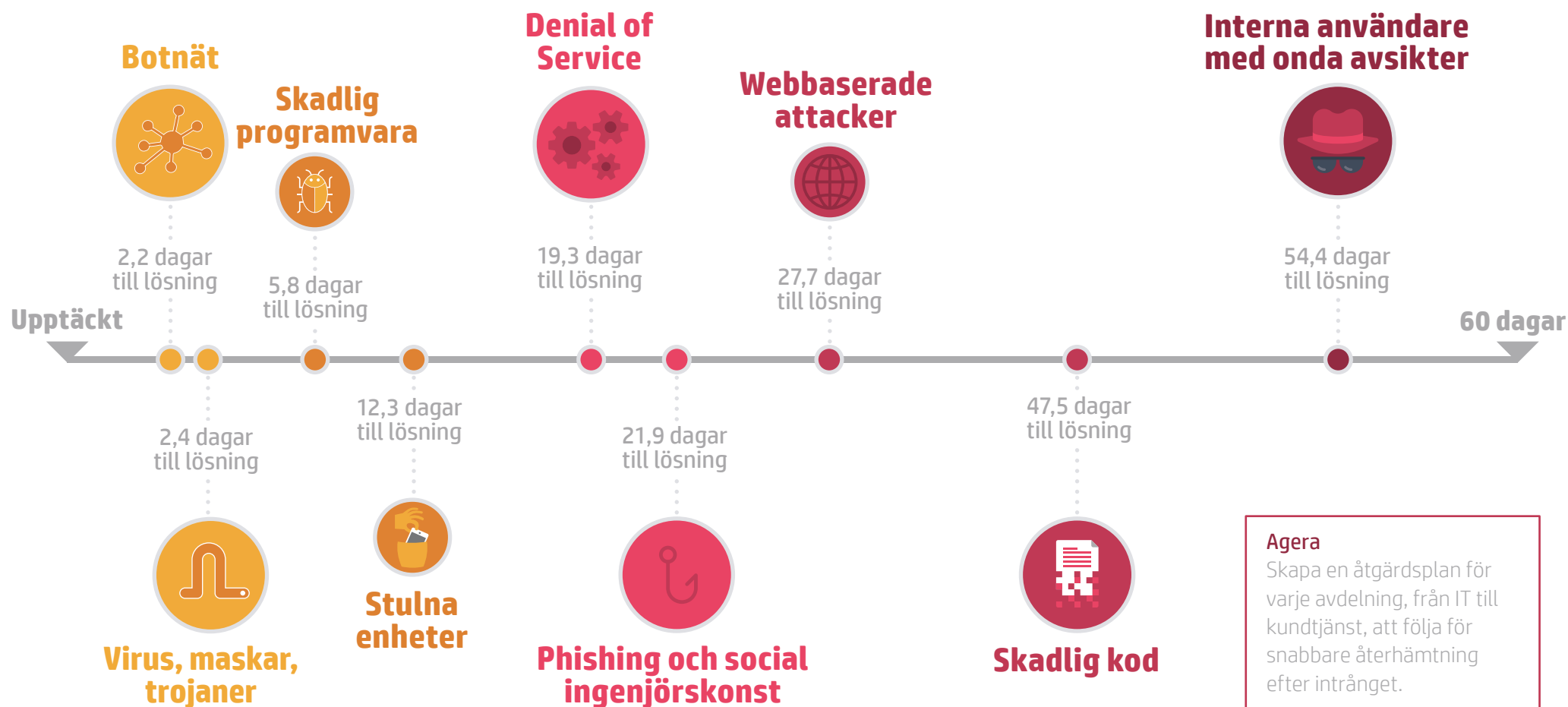
Källor: ¹⁴ <http://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12?IR=T> ¹⁵ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

¹⁶ <https://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/> Stat is \$7.21m – have converted to £

¹⁷ <https://www.gov.uk/government/news/two-thirds-of-large-uk-businesses-hit-by-cyber-breach-or-attack-in-past-year>

DATABROTT: ÅTERHÄMTNINGSTIDEN

Hur lång tid tar det för att reparera skadan av ett dataintrång?
Ponemon-institutet¹⁸ sätter den genomsnittliga tiden vid 46 dagar, en potentiellt förlamande siffra för små och medelstora företag



HUR DU SKYDDAR VERKSAMHETEN MOT CYBERBROTT

Viktiga råd och strategier för verksamhetens cybersäkerhet

Här följer sex vanliga mål för hackare att angripa och vad du kan göra åt dem idag.



Kunddatabaser



Molntjänster



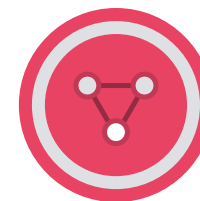
Personalens smarta
telefoner och plattor



Anställdas
misstag



Sakernas
internet



Nätverksgrindar

Vi arbetar allt mer digitalt i en värld där data representerar ett större värde än någonsin tidigare och databrott begås på många sätt. Databrottslingar är ofta på jakt efter information och

med fler uppkopplade enheter på arbetsplatsen – från smarta mobiltelefoner och plattor till WiFi-skrivare – finns ett växande antal angreppspunkter för hackare att inrikta sig på.

1 KUNDDATABASER



Ekonomiska uppgifter är långt ifrån det enda målet för angripare – information som namn och e-postadresser kan användas för identitetsstöld, skräppost eller för att hacka andra konton.

En morot för seriösa hackare är att bryta sig in hos företag med ännu större verksamheter. Du skulle kunna likna det med ett inbrott i en järnhandel där tjuvarna försöker komma åt källarväggen som gränsar till kassavalvet i banken intill.

När angriparen har tagit sig in i det mindre systemet har de en bättre position för att komma åt kunders data som förvaltas av det större företaget. Hur skulle din kunddatabas kunna bli utsatt? Virus, maskar och trojanska hästar – som laddas ner via infekterade webbplatser eller e-post – kan innehålla den kod som en hackare behöver för att komma åt och stjäla data.

Hur du skyddar dina kunders data

- Använd säkerhetsprogram som är avsedda för företag och som skyddar nätverk, e-post och klientenheter.
- Uppdatera alltid ditt säkerhetsprogram för att blockera ny skadlig programvara.
- Ladda ner programuppdateringar för dina systemprogram, då äldre program kan innehålla sårbarheter som hackare kan utnyttja.

2 MOLNTJÄNSTER



Hur du skyddar dina kunders data

- Kryptera din viktigaste information med verktyg som PKWARE:s Smartcrypt-teknik, där åtkomstpolicyer tillämpas för att bestämma krypteringens komplexitet. På det sättet ser berättigade användare de uppgifter de förväntas se, medan ej berättigade användare inte ser någonting.
- Skapa ett starkt lösenord för ditt molnkonto. Definiera i inställningarna för ditt molnkonto exakt vem som ska ha tillgång till dina uppgifter och vad de kan göra med dem.
- Kräv tvåfaktorsautentisering – exempelvis en mobiltelefonkod och ett lösenord – för att göra ändringar av molndata som nedladdning, radering eller flyttning av filer.

Molnet har blivit en del av infrastrukturen som företag fastnat för.

IDG Cloud Computing Survey 2016¹⁹ fann att 70 % av företagen har förlagt åtminstone någon del av infrastrukturen i molnet, medan Tripwire fann att 90 % använder molnet för infrastruktur och/eller datalagring – inklusive affärskritisk data.²⁰

Säkerhet är givetvis ett bekymmer, men faktum är att data normalt är säkrare i molnet – när de lagras på servrar utanför företagets byggnader av ett företag vars anseende byggs på säkerheten.

Det är därför som 64 procent av företagen som undersöktes av Tripwire ser molnet som säkrare än gamla system.

Lyckligtvis är denna förhoppning inte grundlös – enligt BIS-undersökningen 2015,²¹ utsattes bara sju procent av företagen (stora och små) för allvarliga brott mot sina molntjänster, och dessa beror i allmänhet på åtkomstillstånd eller olämpliga lösenord. Men även ett säkert moln kräver robust intern säkerhetsledning. Tänk bara på Sonys huvudentré.

86 % av företagen använder eller planerar att börja använda molnet.

Källor:

¹⁹ <https://www.scribd.com/document/329518100/IDG-Enterprise-2016-Cloud-Computing-Survey>

²⁰ <https://www.tripwire.com/state-of-security/security-data-protection/enterprise-impressions-of-cloud-security-in-2016/>²⁰

²¹ 2015 Small Business Survey. Department for Business, Innovation & Skills

3 PERSONALENS SMARTA TELFONER OCH PLATTOR



Många använder sina egna enheter för kontorsuppgifter.

En BYOD-policy (Bring your Own Device) för företaget är ett effektivt sätt att utnyttja mobiltelefoner som anställda redan äger. Detta är en ökande trend och 53,2 procent av företagen implementerar BYOD-policyer inom de kommande två åren.²² Dessa utrustningar kan dock vara ett mål för angripa.

En av fem Android-appar uppskattas innehålla någon form av inkräktande programvara som kan överföras till företagsfiler och system för att övervaka aktiviteter eller stjäla information.

Detta hot ökar och 64,9 % av företagen uppger att mängden hot som riktas mot deras mobilenheter har ökat.²³

Anställdas stulna mobiltelefoner kan också, utan innehavarens vetskap, öppna möjligheter för intrång. En telefonjuv säljer en enhet till en köpare på svarta marknaden som i sin tur kan finna information för att begå intrång på offrets företag, eller ta sig in i en större klients system. Företagen graderade sin förmåga till försvar mot säkerhetshot som härstammar från mobila enheter till 3,54 av 5. Det var den lägsta graderingen bland de tänkbara ursprung för hot som de tillfrågades om.²⁴

Hur man skyddar personalägda enheter

- Installera ett verktyg för upptäckt av hot, exempelvis Duo:s X-Ray för Android-enheter för att underlätta spårning av infekterade appar och misstänkt kod.
- Be anställda att aktivera fjärrrensning (finns gratis för Android, iPhone och Windows Phone med abonnemang på BlackBerry) så att känslig data, såväl privat som företags, i händelse av förlust, kan raderas.
- Be anställda att aktivera enhetskryptering på sina smarta mobiltelefoner för att skydda data (aktiverat som förval på nya iOS och Android-telefoner).

4 ANSTÄLLDAS MISSTAG



Hur du hjälper personalen

- Utbilda personalen om bästa metoder inom cybersäkerhet och erbjud regelbunden uppdatering för medvetenhet om de senaste hoten.
- Utveckla ett säkerhetsprotokoll skräddarsytt för din verksamhet och de typer av data som behandlas.
- Skapa en grupp som kommunicerar policyn för cybersäkerhet till anställda och samarbetsparter.

Den mest grundläggande faktorn i cybersäkerhet är en bra lösenordspolicy, men ändå berodde 31 procent av intrången under 2015 på personalrelaterade händelser.

Angripare utnyttjar ofta mänskliga misstag när det rör sig om avslöjande av svaga lösenord,

stöld av dokument som e-postas via oskyddade anslutningar eller nätfiske riktat mot en viss anställd.

5 FÖRBERED FÖR "SAKERNAS INTERNET"



Undersökningsföretaget IDC antar att antalet enheter som ansluts till internet kommer att öka från 13 miljarder till 30 miljarder fram till år 2020.²⁵

Medan kontorsdatorer skyddas åtminstone med lösenord och i bästa fall med säkerhetsprogramvara, är skrivarköer och utskriftsjobb inte skyddade med liknande säkerhetsprotokoll.

Sådana oskyddade skrivare – och annan nätansluten utrustning – kan utsättas för "sniffer-program" som kan logga utskriftsjobb lika väl som nätverkstrafik, användarnamn och lösenordsinformation, och skickas tillbaka till de kriminellas server.

Det är värt att notera här att det mycket omskrivna Dyn-

intrånget enligt uppgift länkades till ett nätverk av webbaktiverade övervakningskameror tillverkade av ett enda företag, XiongMai Technologies. Enligt säkerhetsföretaget Flashpoint.

Detta illustrerar att varje enhet i ditt nätverk är en ingång och ditt nätverk är bara så säkert som din minst säkra enhet. Ungefär 97 % av företagen har säkerhetsrutiner för stationära och bärbara datorer, 77 % för mobila enheter, men bara 57 % har säkerhetsrutiner för skrivare.²⁶ Det enda sättet att förbli säker är att alla företag har säkerhetsrutiner för varje enhet.

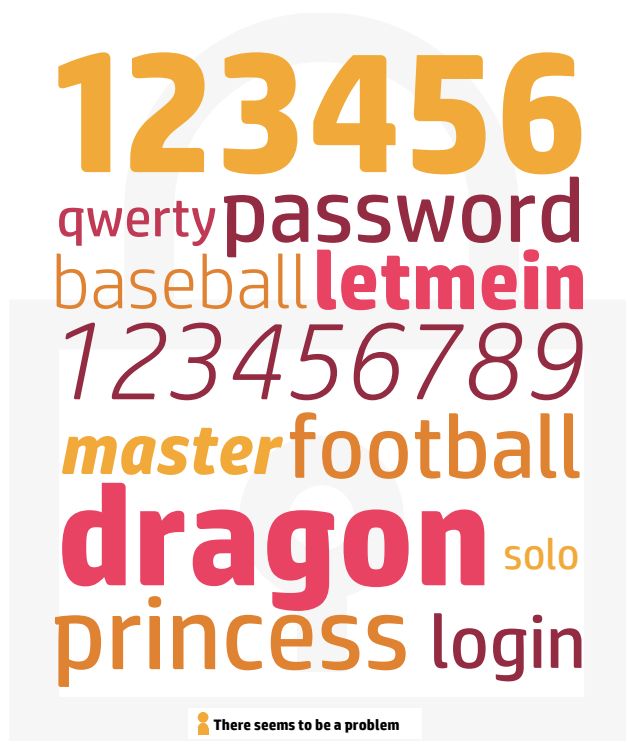
Hur man förbereder sig för "Sakernas internet"

- Ta bort eller avaktivera onödig funktionalitet på utrustningen eftersom fler funktioner kan skapa fler öppningar för angripare.

LÖSENORD OCH RANSOMWARE

De vanligaste lösenorden

I början av 2013 hade en Ars Technica-reporter, som inte var någon internetbrottsling och inte hade någon som helst erfarenhet av att bryta sig in i lösenordskyddade system, knäckt 8 000 av mer än 16 000 krypterade lösenord på en dag*. Så vad har dessa extremt vanliga lösenord för chans mot en bestämd hackare?



Vad är ransomware?

Internetbrottslingar har i allt högre grad vänt sig till ransomware, en form av skadlig programvara som kapar system, vilka sedan kan låsas upp endast efter leverans av en lössumma i bitcoin. Tusentals drabbades av ett utbrott år 2013 av en trojan med namnet Cryptolocker, som uppmärksammades av Storbritanniens nationella brottsbyrå och dess nationella cyberbrottsenhet. Här kommer en närmare titt på hur dessa typer av attacker fungerar.



1. Installation

Den skadliga koden arbetar sig in i datorn efter en oavsiktlig nedladdning, via e-post eller en skadlig webbplats.



2. Larmar sina huvudkontor

Ransomware (utpressningsprogramvara) ansluter med sin hemserver för att skapa en krypteringsnyckel.



3. Krypterar dina filer

Ransomware skannar filerna i ditt nätverk och krypterar dem, vilket gör dem otillgängliga.



4. Utpressning

Ett meddelande dyker oftast upp på användarens dator som visar en tidsgräns och en summa att betala för att dekryptera filerna innan de raderas.



5. Betalning

Företagsägare kan köpa en digital valuta, som bitcoin, för att med hjälp av den överföra summan till hackaren, som förhoppningsvis dekrypterar filerna.

6 NÄTVERKSGRINDAR



När angripare vill ta sig in i ett nätverk kan de aktivera en DDoS-attack – tusentals datorer infekterade med skadlig programvara samverkar för att skapa så mycket skräptrafik att nätverket slås ut.

Vid DDoS-attacker vill man ofta distrahera administratörerna med ett "fruset" system medan data stjäls eller skadlig programvara installeras för att förbereda framtida angrepp. Vissa DDoS-attacker är också en konsekvens av att "script kiddies" eller "nybörjarhackers" vill blockera webbplatser, bara för att de klarar av det. Även ett kort avbrott på några timmar kan få stora konsekvenser för ett företags resultat eller anseende.

TIPS:

Investera i hårdvara som erbjuder inbyggt skydd, exempelvis avancerad autentisering och krypteringsverktyg.

Hur du skyddar ditt nätverk

- Bygg upp system som kontrollerar trafiken in i och ut från nätverket. En plötslig topp kan tyda på en attack och en konstant men oväntad aktivitet kan tyda på att en trojan rapporterar data tillbaka till moderskeppet.
- Filtrera all trafik så att endast trafik som krävs för att stödja verksamheten kommer in i nätverket.
- Se till att varje router, switch eller annan nätverksutrustning fungerar med samma grundprogramvara och funktionalitet och ladda alltid ner programvaruuppdateringar.

FRAMTIDENS CYBERSÄKERHET FÖR FÖRETAG

I verksamheter som är allt mer internetberoende, ökar kraven på ett robust försvar för cybersäkerhet.

Numera tar anställda med sig sina egna enheter till arbetet. Företag implementerar molnbaserade plattformar och anlitar leverantörer för viktiga tekniska tjänster. Och allt fler arbetar nu på distans. Säkerheten på nätet blir en tuffare utmaning när du varken har kontroll över enheten, infrastrukturen eller arbetsmiljön.

Samtidigt har vi med den mobila teknikens intåg fått lära oss att arbete kan utföras när och var som helst. Man kan jobba på ett kafé lika väl som på ett kontor. Vi använder offentliga WiFi-nätverk för hantering av oerhörda mängder privat och arbetsrelaterad information – ofta via smarta mobilenheter med bristande säkerhet. Kriminella är väl medvetna om detta skifte.

Säkerheten blir lidande när vi inte är uppmärksamma på omständigheterna för arbetet.

I framtiden kommer det att betyda betydligt mer än att installera virusprogram på våra enheter eller att uppdatera lösenorden en gång i halvåret. Företag måste vidga perspektivet till förstärkta säkerhetslösningar som fungerar lika bra på distans som de gör i en kontorsmiljö med övervakning av en IT-administratör

För morgondagens utspridda organisationer måste cybersäkerheten grundas på avancerad analys som isolerar ovanliga beteenden och skiktad säkerhet som skyddar alla åtkomstpunkter.

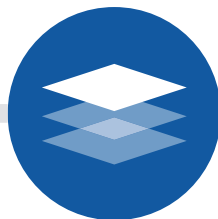


FRAMTIDENS CYBERSÄKERHET FÖR FÖRETAG



Analysverktyg: säkerhetsdetektiven på internet

Även om din webbplats inte belastas av intensiv trafik, kommer den att ha mönster. Med hjälp av analysverktyg som mäter och loggar aktiviteter kan man lättare diagnostisera när något inte stämmer. Dessa verktyg spårar och dokumenterar normalt beteende först för att sedan upptäcka avvikelser. När något har upptäckts kan administratörer börja agera och avstyra attacker innan någon chans ges att ställa till problem.



Lager: håller angripare ett steg bakom

Säkerhet i lager omnämns ibland som "försvar i djupled" och skyddar varje åtkomstpunkt i flera lager. Vanliga angreppssätt är utökade SSL-certifikat för validering som försvårar förfalskning av inloggningsuppgifter för intrång på ett säkert nätverk. Utöver detta kan även skyddet förstärkas med multifaktorauslösnings, som kräver att angripare avslöjar mer än bara ett lösenord för att lyckas.

Oavsett vilken specifik teknik som utnyttjas, är principen bakom skiktad säkerhet att varje känsligt område i verksamhetens nätverk på något sätt stängs av. Dina användare och samarbetspartner kanske måste ägna något mer tid för att tillgå viktiga data, men den tid och kraft som offras bör mer än väl kompenseras av trygghet för verksamheten.



Agera nu

Det bästa försvaret är att investera i internetsäkerhet och utbildning. Börja med en genomgång av dina system och din infrastruktur. Gör du tillräckligt? Vad kan du göra bättre?

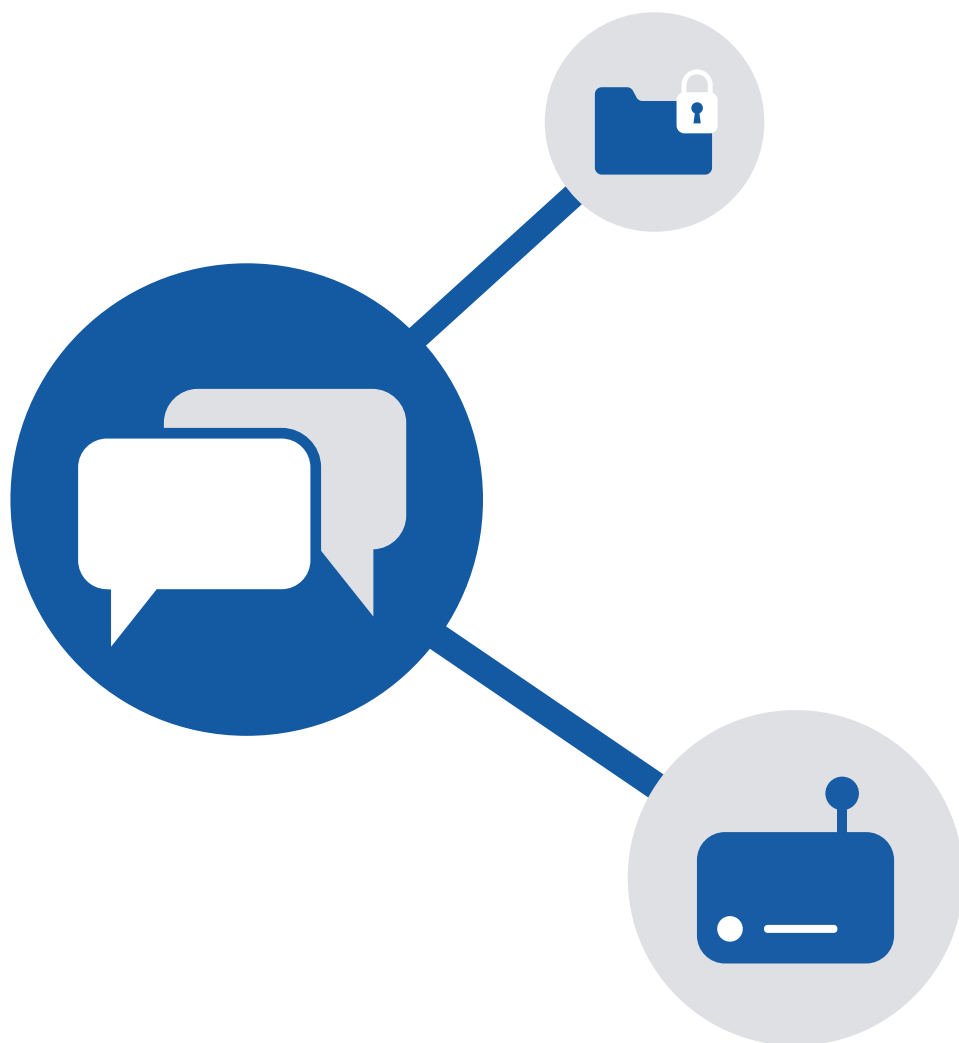
Avslutningsvis kan du även ringa våra experter här på HP Inc. Vår samlade kompetens är inriktad på att ligga steget före hoten, inte bara att svara på dem. Besök oss på [HP.com](https://www.hp.com) för att läsa mer.

TIPS:

Spåra och dokumentera normalt beteende först för att sedan upptäcka avvikelser.

ÖVERVÄGANDEN FÖR KLIENTSÄKERHETEN

Att skydda varje enskild enhet i nätverket



I säkerhetsutredningar som utfördes av Spiceworks²⁷ fann man att den viktigaste källan till säkerhetshot mot företag var:

- Bärbara och stationära datorer: 81 % externa och 80 % interna
- Mobila enheter: 36 % externa och 38 % interna
- Skrivare: 16 % externa och 16 % interna

Mot vilka av dessa hot är det mest angeläget att vara skyddad? Samtliga, är det enkla svaret. Detta kan förefalla solklart, men ett alarmerande antal företag väljer fortfarande vilka enheter de vill skydda.

HPs sätt att se det är att varje enhet som ansluts till ditt nätverk måste vara skyddad. Enkelt uttryckt: Ditt nätverk är bara så säkert som din minst skyddade enhet.

Med intuitiv logik kan du komma fram till att säkring av en ansluten skrivare inte är lika viktigt som att skydda alla dina bärbara datorer. Men risken är lika stor. Hackare är kända för att inrikta sig på saker som skrivare eller alla smarta enheter som är anslutna till nätverket. Orsaken är att de vet att dessa enheter normalt inte är särskilt väl skyddade, men ger samma nivå av åtkomst till ditt nätverk.

HP VISAR VÄGEN I ETT NYTT LANDSKAP

Cyberäkerhet förändras. Vi har verktygen för ditt försvar.

Det finns inga enkla knep för cybersäkerheten. Ett robust försvar måste byggas på ett angreppssätt med hänsyn till många faktorer innefattande nätverk, enheter och människor. Välja rätt metoder och lösningar är en god start.

På HP kommer säkerheten först. HP Premium Elite-serien inkluderar marknadsledande säkerhetsfunktioner som inte finns tillgängliga någon annanstans, som HP SureStart – världens första självläkande BIOS.

HP utrustar sina produkter med:

- **HP WorkWise:** Med hjälp av Bluetooth låses maskinen automatiskt när du lämnar den, och låses upp när du kommer tillbaka.
- **Biometrisk säkerhet:** Igenkänning av ansikte och fingeravtryck ger åtkomst endast för biometriskt autentiserade användare.
- **HP SureView-skärmar**:** Den mörklägda skärmen hindrar att andra ser din skärm och skyddar konfidentiell information när du arbetar på resande fot.
- **HP SureStart självläkande BIOS:** HP Elite kontrollerar sin BIOS var 15:e minut. Vid upptäckt av en anomali återställer den datorn till sitt ursprungliga tillstånd och stöter ut eventuella inkräktare.**

HPs Elite-serie kan inte att skydda din verksamhet på egen hand. Men de ger goda förutsättningar. Läs mer om den kompletta HP Elite-serien [här](#).

För enkel åtkomst till varje enhet och den service ditt företag behöver, kolla in HP Device as a Service. Du kan välja en enhet och tillbehörsmix som är lika unika som dina krav är, och alla fjärrstyrs, optimeras och underhålls av HP. Läs mer om HP Device as a Service [här](#).

* Valda modeller

** Baserat på PC-konkurrenter per den 1 december 2016 med över 1 miljon enheter årligen med detektering och självläkning på BIOS-nivå, attackdetektering i runtime-minne, BIOS konfigurations- och policyskydd

ORDLISTA OCH FORTSATT LÄSNING

Verktyg för åtkomststyrning

Botnät:

Avser normalt en typ av automatiserat program utvecklat för att komma åt och styra internetanslutna datorer utan användarens vetskap. Datorerna infekteras ofta av skadliga program. Hackare använder botnätsprogram för att släppa loss en **DDoS-attack** på en webbplats.

Brandväggstekniker:

Ett annat brett begrepp som avser en typ av utrustning som med algoritmer och annan teknik blockerar obehörig trafik och användare från att ansluta till nätverk. **Nästa generations versioner** av dessa utrustningar klarar att kombinera funktioner som tidigare endast kunde hanteras av enskilda utrustningar. Upptäckt av intrång till exempel. De går också mot att bli applikationskänsliga och därmed kunna skilja mellan webbftrafik från en implementering från salesforce.com och från en Facebook-sida.

GRC-verktyg:

Avsedda för att hänvisa till breda och samordnade initiativ syftar internt i ett företag till att hantera och styra driften på ett sätt som överensstämmer med bestämmelser, varigenom risker reduceras.

Krypteringstekniker:

Verktyg som gör **data i sig själv oläsbar** utan någon typ av avkodare. Storbritanniens informationskommissionär har under tidigare år pläderat **starkt för** olika typer av kryptering. Senare har regeringen tvingats **backa från sin position inom krypteringsteknik** under påverkan av häftig kritik.

Maskar:

Maskar kan, till skillnad från virus som sprids genom delning av filer som Word-dokument eller Excel-kalkylblad, spridas oberoende av värddokument och kräver därför ingen mänsklig medverkan för att vålla kaos. Snabbmeddelandesystem är välkända källor till spridning av maskar. Skype drabbades av det under 2012.

Nätfiske:

Bedrivs normalt via e-post där angriparen efterfrågar identifierande information i en dialogruta som ser legitim ut.

Omkretskontroller:

En allmän kategori av cybersäkerhetsfunktioner vid den punkt där offentligt internet eller annat offentligt nätverk gränsar till ett privat och lokalt ägt och förvalt nätverk. **Flerlagersteknik och olika enheter** är vanligen inblandade.

Säkerhetsinformationssystem:

Med många olika typer av säkerhetsinformation kan man samla och syntetisera data som är relaterade till hot. Det finns många olika system, från logghanterare till system för upptäckt av nätverksavvikelser.

Skadlig programvara:

En omfattande kategori av programvara som kan vålla skador på och även slå ut system. Virus, maskar och trojaner är exempel på skadliga program. För Ponemon-studiens syften som åberopas i denna e-bok, betraktas skadlig programvara som något skilt från virus och som sägs "ha placerats på en klientenhet och ännu inte infiltrerat ett nätverk".

ORDLISTA OCH FORTSATT LÄSNING

Social ingenjörskonst:

En metod där en angripare försöker tvinga en auktoriserad användare att avslöja otillbörlig information som ger angriparen åtkomst.

Trojanska hästar:

Trojanska hästar ger liknande påverkan som virus eller maskar, men måste installeras av användaren och brukar därför vara skickligt maskerade. Påverkan kan vara många saker från att förändra datorns inställningar till att radera filer och skapa en "bakdörr" som en hackare kan utnyttja senare.

Verktyg för policyhantering:

Verktyg för policyhantering utgör i vid mening en nivå för vad respektive användare har eller inte har tillgång till, och garanterar därmed att policyn följs i hela nätverket. Konsekvens (åtminstone i teorin) garanterar säkerheten.

Verktyg för skydd mot dataförlust:

En omfattande kategori av mjukvara för att övervaka känsliga data och blockera obehörigas försök att komma åt eller kopiera den. Åtkomstpunkten (dvs. klientenheten) kan skyddas genom olika angreppssätt medan nätverk skannas över eller i ett filsystem. Gartner fick denna marknad att **växa med 25 procent** under 2013.

Virus:

Skadlig kod som kan fortplanta och sprida sig genom ett nätverk.

Webbaserade attacker:

Oftast ingår omdirigering av webbläsaren till en skadlig plats i en webbaserad attack.

