Vitbok för företag

Säkerhet börjar med användaren

Det gäller att prioritera klientsäkerhet

Presenteras av

Sammanfattning

82 % av organisationerna har upplevt ett hot eller en överträdelse mot cybersäkerheten under de senaste 12 månaderna.[1] Cyberbrotten ökar i attackfrekvens, svårighetsgrad och kostnad.

Paradigmet att förebygga och skydda säkerheten – att försvara nätverkets yttre gränser med brandvägg – är över. Att upptäcka och reagera är mycket effektivare.

Men fördelningen av IT-budgetar speglar inte förändringarna i cybersäkerhet. 77 % av utgifterna läggs fortfarande på att förebygga och skydda.[2] Endast 36 % av cheferna för IT-säkerhet tycker att de har gott om budget för effektiv klientsäkerhet.[3]

Ett robust dataskydd är möjligt. Med rätt teknik – med säkerhetslösningar som upptäcker och reagerar ända ner till enskilda enheter – rätt strategi och tillräckliga resurser, kan organisationerna skydda sig från cyberbrottslighet.

Om man inte ökar investeringarna i cybersäkerhet, och inte justerar investeringarna mot verkligt och effektivt försvar, kommer det leda till en ökad förekomst av säkerhetsöverträdelser – vilket innebär en ökad kostnad för organisationen.

Introduktion

Cybersäkerhet i en tid av amorfa nätverk
60 % av IT-cheferna känner att den alltmer avancerade cyberbrottligheten och den ökade volymen av dessa brott går snabbare än deras försvar. 80 % av säkerhetscheferna uppfattar hotet från avancerade långvariga hot (”Advanced Persistent Threats”, APT:er), kriminella företag, statligt stödda hackare och hacktivister som växande och den viktigaste utmaningen för IT-säkerhet.[4]

De har inte fel. I Storbritannien har regeringen uppskattat den ekonomiska kostnaden för cyberbrottslighet till 280 miljarder SEK, en siffra som är ”betydande och sannolikt kommer att växa”, med en förlust på 217 miljarder SEK för företagen.[5] I Ponemons 2016 State of the Endpoint Report, redovisade 78 % av företagen en ökning av svårighetsgraden av skadliga attacker, från 47 % år 2011.

Men fokus på externa hot är något missriktat och kan leda till en orealistisk koncentration av resurser som försvarar och förebygger skyddet för den yttre gränsen.

Även om externa attacker – virus, skadlig programvara, phishing – är vanligare är insiderattacker dyrare.[6] Dessutom kommer många av dessa externa attacker från svagheter internt; försumliga medarbetare som ignorerar säkerhetsprotokollen, enheter utan säkerhet som ansluter till nätverket – något som 81 % av de tillfrågade i Ponemons undersökning identifierade som det största hotet mot IT-säkerheten.

Detta kommer att bli ännu mer sant med tiden. Användaren är den svagaste noden i alla nätverk, och med ökningen av BYOD, distansarbete och Sakernas internet (IoT), förökar sig enheterna. Detta innebär att antalet ingångar för hackare också förökas.

Långt från de dåvarande kontrollerade nätverken av datorer hopkopplade med Ethernet, har företagsnätverken blivit svårare att överblicka, en härva av enheter både för affärsbruk och personligt bruk med tillgång till data genom flera WiFi-knutpunkter både på plats och utanför.

Men situationen är inte hopplös. Det betyder helt enkelt att man måste anta en ny strategi för cybersäkerhet. Nya strategier som reagerar på förändringen i cyberbrottslighet. Ny teknologi som är kapabel att avleda alltmer sofistikerade, växande hot.

I den här vitboken kommer vi att undersöka arten och omfattningen av hotet – för att bättre lära känna vår fiende – innan vi tar itu med frågan om hur vi hanterar cybersäkerheten i en tid av multipla enheter, osäkra nätverk och molnet.

[1] HPI Printer Security Research 2016 (Spiceworks)
[2] PAC Incident Response Management 2015: https://www.pac-online.com/download/19443/155514
[3] Ponemon 2016 State of the Endpoint Report
[4] IBM CISO Assessment 2014
[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[6] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic

Hotets omfattning

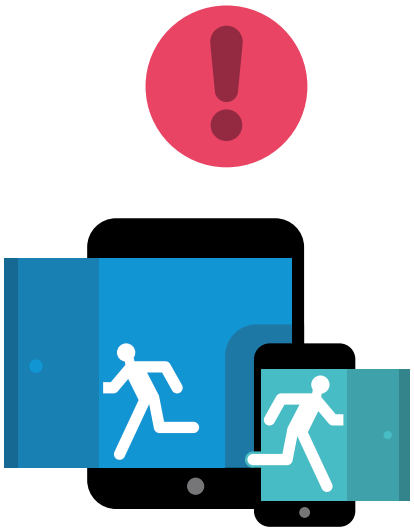
Ett genomsnittligt informationsläckage kostar företagen 7.3 miljoner SEK att återhämta sig från, med ytterligare en förlust på 13 % i intäkter. I genomsnitt skulle det ta en organisation nio veckor att återhämta sig.[7]

I HP Printer Security Report 2015 uppgav cirka 85 % av de tillfrågade företagen att de hade upplevt ett hot mot säkerheten/överträdelse de senaste 12 månaderna. 80 % av de tillfrågade IT-specialisterna bedömde att hotet kommer att öka under de närmaste tre åren. [8]

Cyberbrott kostar reella pengar. Förlorat värde från det som har stulits eller skadats. Förlorade intäkter från skadat anseende och förlorad produktivitet. Förlorade resurser som läggs på återhämtning – supportavdelningens tid, införande av nya säkerhetsregler, personalförluster och andra interna lösningar. Böter och straffavgifter från regleringsmyndigheter. En nedgång i aktiekursen.

Hotet kommer bara att växa tillsammans med antalet enheter som är anslutna till nätverket. Gartner förutspår att det, tack vare Sakernas internet (IoT), kommer att finnas 11,4 miljarder anslutna enheter år 2018, en ökning med 6,4 miljarder från år 2016. År 2020 kommer mer än 25 % av de identifierade attackerna i företag vara IoT-relaterade, men IoT kommer att omfatta mindre än 10 % av säkerhetsbudgeten.[9]

Hotet från cyberbrottslighet är stort, och blir allt större.



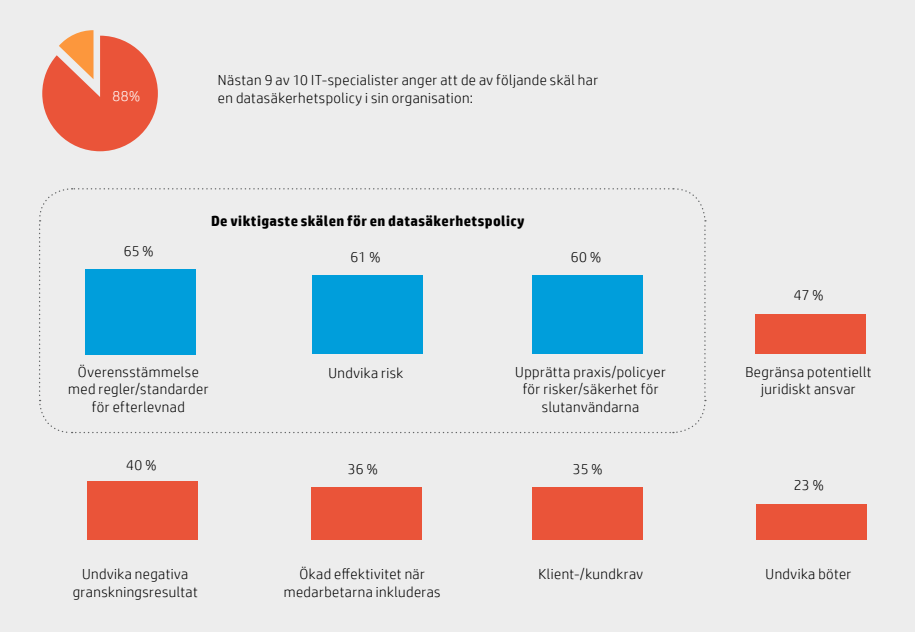
Hotets form

Affärsverksamheter angrips av otaliga cyberattacker varje dag. De flesta är virus- och skadliga programvaruattacker på låg nivå. 99 % av de organisationer som Ponemon år 2016 frågade hade upplevt skadlig programvara under de senaste 12 månaderna. Externa webbaserade attacker som dessa är relativt godartade och kostar organisationerna i genomsnitt 37000 SEK.[10]

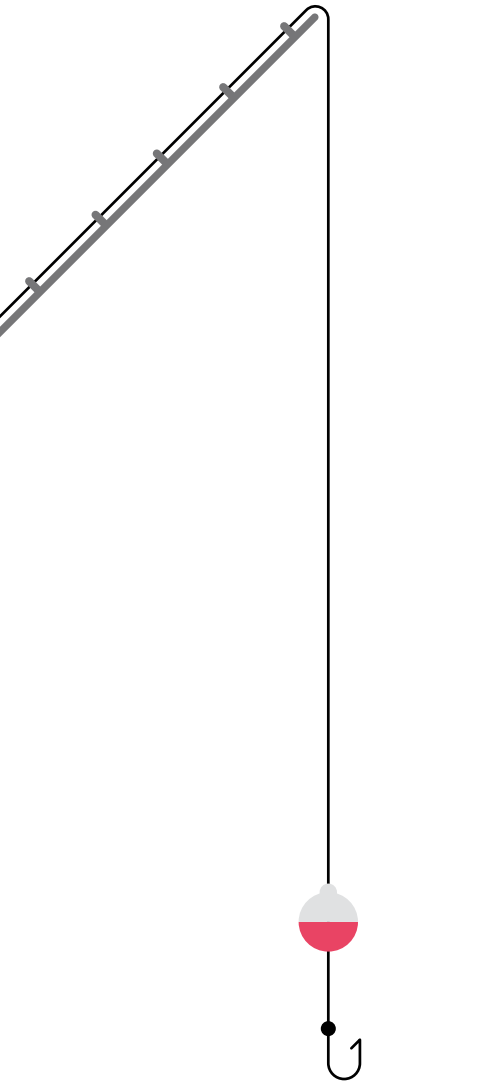
Men allvarligare attacker blir allt vanligare. 51 % av de år 2015 tillfrågade organisationerna hade upplevt överbelastningsattacker (Direkt Denial of Service, DDoS), som kan vara förödande och kostar i genomsnitt 1 miljon SEK. Ännu mer oroväckande är att 35 % hade upplevt en skadlig insiderattack, till en genomsnittlig kostnad på 1,2 miljoner SEK.[9]

Den framväxande bilden visar hänsynslösa mindre angrepp utifrån, och mer sällsynta men förbluffande troliga stora attacker som förmodligen har orsakats av insiderförsummelse, kanske även med illvilja. 62 % av organisationerna hade upplevt nätfiskeattacker och sociala manipuleringsattacker, som utnyttjar anställdas svaghet med en genomsnittlig kostnad av 688000 SEK.[11]

En separat undersökning av Spiceworks – på uppdrag av HP – analyserade attacker som 90 brittiska organisationer erfarit under åren 2014–2015.[12]



[7] NTT Security Risk:Value Report 2016
[8] HP 2Printer Security Report 2015
[9] http://www.gartner.com/newsroom/id/3291817
[10] https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-8392enw.pdf
[11] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic
[12] HPI Printer Security Research, Spiceworks 2016



Hur överträdelser inträffar

Rubrikerna skildrar initiativrika hackare som lyckas bryta sig in i regeringarnas och företagens avancerade, säkra nätverk, men verkligheten är oftast mer sober.

Virus kan utnyttja kompromissade nätverk, men skadlig programvara kräver vanligtvis någon form av användarfel. Nätfiskeattacker och sociala manipuleringsattacker är beroende av dessa. Stora DDoS- och informationsstöldsattacker är ofta också ett resultat av användarens försummelser.

Den nu ökända hackningen av Dropbox sägs vara resultatet av en slarvig Dropbox-anställd som använde samma lösenord för interna system som för sitt Linkedin-konto.[13] Den påstådda ryska hackningen av Democratic National Committee (DNC) hände tydligen tack vare John Podesta, en före detta rådgivare till Hillary Clinton, som klickade på en länk i ett nätfiskemejl som var felaktigt flaggat som ”legitimt” av en medhjälpare.[14]

Hackare behöver inte aktivt stöd för att lyckas. Lika farligt är okunnighet om, eller likgiltighet för, säkerhetsprotokoll. Ett allt större hot är anställda som kommer med sina egna enheter till arbetet och använder kommersiella molnapplikationer. Båda betyder att osäkra element till ett annars säkert nätverk; utom kontroll för företagets IT och skapar en sårbarhet som inte granskas.

För det mesta behöver hackare inte använda avancerade algoritmer eller den senaste teknologin. De behöver bara någon som är lite slarvig.

Brandväggen är sönder

Grundstenen i cybersäkerhet har tills nyligen varit antivirus- och brandväggsprogram. Förebygga och skydda. Genom inrättandet av en skyddande yttre gräns. I den nuvarande arbetsmiljön är det helt enkelt inte en trovärdig strategi.

81 % av de som Ponemon frågade säger att mobila enheter på deras nätverk har varit mål för skadlig programvara. Andra ökningar av säkerhetsrisker inkluderar anställdas användning av kommersiella molnapplikationer – citerades av 72 % av de tillfrågade – BYOD (69 %) och anställda som arbetar från hemmakontor och externa platser (62 %).[15]

Mer förenklat sagt var en brandvägg relevant när nätverksadministratören kunde kontrollera vilka enheter som var anslutna. Men i en tid då de anställda tar med sina egna enheter till arbetet – ofta flera, ofta utan IT-kunskap – och allt fler arbetare är distansanslutna, kan man helt enkelt inte skydda perimetern. Varje enhet som inte granskas är en sårbar slutpunkt som hackare kan utnyttja.

[13] https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach
[14] https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0
[15] Ponemon 2016 State of the Endpoint Report

HPs perspektiv: Att gå bortom nätverkssäkerheten

Michael Howard, HP:s globala chef för säkerhetspraxis, om säkerställande av klientsäkerhet

En viktig och aktuell fråga är att företagen kämpar för att säkra varje enhet på grund av otillräcklig insikt och kunskap om vissa enheter och de risker de för med sig. De känner sig säkra bakom en brandvägg, trots att detta inte längre är tillräckligt för att skydda mot en attack. Säkerhetsteam måste känna till alla enheter inom infrastrukturen och se till att varje enhet har flera lager av skydd för att skydda sig mot allt mer sofistikerade attacker.

Det är viktigt att säkerhetsteam undersöker alla delar av IT-infrastrukturen i sin verksamhet och bygger ett extra lager av skydd ovanpå standardnätverkets perimeter. Enbart brandväggar klarar inte sofistikerade attacker och en försvarspolicy med flera skyddslager vid varje klientenhet är ett måste för att säkerställa att affärsverksamheten efterlever lagstadgade krav och kan undvika kostsamma böter.

HP:s policy är att med varje ny lösning, tjänst eller produkt som de utvecklar, kommer säkerheten att vara det första de tittar på. Utvecklingsteamen vet att de måste besvara säkerhetsfrågorna och de måste veta hur de ska placera dem i nätverket på ett säkert sätt.

Mer än någonsin tidigare bör säkerheten komma först, inte som ett tillägg. Det har i åratal varit HP:s policy.

Säkerhet i lager

En ny strategi för cybersäkerhet måste vara i flera lager.
Nätverkssäkerheten är fortfarande viktig, men den måste formas av åtskilda nätverk. Många överträdelser sker via ett första inträde som ger tillgång till hela systemet. Tänk på John Podestas felsteg med nätfiske. Det är viktigt att avgränsa känslig information genom flera lager av åtkomst, så att den som stjäl en nyckel inte kan erövra hela slottet.

Enheterna måste redovisas. En kärnfråga för IT-chefer är att säkerställa att varje enhet som är ansluten till nätverket är skyddad av regelbundet uppdaterade säkerhetsprogram – mot virus, skadlig programvara och spionprogram – och att de regelbundet skannas för att upptäcka avvikelser. Det är bättre att använda enheterna själva som sensorer, vilka samlar information i realtid för att varna om eventuella överträdelser mot nätverksperimetern som de är en del av.

Fullständig säkerhetsstyrning måste finnas på plats, där varje anställd är utbildad i cybersäkerhet. Mänskliga misstag – att klicka på fel länk eller att ansluta med en konsumentenhet – är hot nummer ett mot nätverket. De mänskliga misstagen kan reduceras med utbildning.

Enhetssäkerhet

Det största problemet som modern cybersäkerhet kanske konfronteras med är kontroll över vilka enheter som har tillgång till nätverket.
Den första och enklaste lösningen som man oftast genomför är att ha separata WiFi-nätverk för gäster och anställda, så att osäkra externa enheter inte har tillgång till huvudnätverket. Detta går hand i hand med utbildning av anställda i att använda detta nätverk med deras personliga enheter.

Den andra är att se till att du har kontroll över anställdas enheter. Denna angelägenhet måste speglas i företagets policy om BYOD eller CYOD, och är ett starkt argument till fördel för CYOD – som ger mer kontroll över vilka enheter som används och väljer de som har bättre säkerhetsfunktioner, hur de har konfigurerats, samt administreringen och övervakningen av dessa enheter.

Att använda en av våra HP-datorer i Elite-serien, till exempel, är att föredra framför en bärbar dator i budgetklass. Alla HP Elite-datorer har HP SureStart-teknologi som kontrollerar BIOS var 15:e minut och återställer maskinen till sitt ursprungliga tillstånd vid detektering av en avvikelse och blockerar oönskade inkräktare. Tack vare den här funktionen – och många fler – förklarades i vår HP Elite 800-serie nyligen förklarats som ”de säkraste datorerna i världen”. Men det är föga troligt att de anställda själva äger en HP Elite-dator.

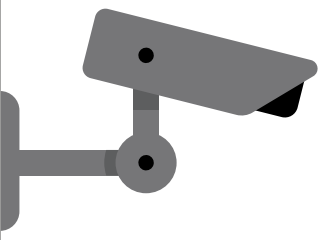
Anställda föredrar ofta att använda sina egna enheter av två skäl:
1. Tekniken i en konsumentenhet är ofta bättre än den som erbjuds på arbetsplatsen
2. Anställda föredrar att använda teknik som de är bekanta med

Genom att erbjuda en CYOD-policy med bra resurser, som ger de senaste enheterna en regelbunden uppdateringscykel, kan organisationer erbjuda bättre enheter än vad de anställda har, och upprätthålla större säkerhetskontroll över dessa enheter. Detta är vad vi erbjuder med vår HP Device as a Service (DaaS).

Det är mycket viktigt att inkludera alla enheter i säkerhetsstrategin, även de som ofta glöms bort. I en undersökning genomförd av International Data Corporation (IDC) svarade 80 % av de tillfrågade att IT-säkerheten är viktig för deras affärsverksamhet, men endast 59 % ansåg att utskriftssäkerheten är viktig, även om mer än hälften hade upplevt en säkerhetsöverträdelse som var relaterad till utskriftssäkerhet under de senaste 12 månaderna. Detta är en tydlig blind fläck.

Innan man införde en säkerhetspolicy för utskrifter var det genomsnittliga antalet säkerhetsöverträdelser 9,9 per år med en genomsnittlig kostnad på 4,1 miljoner SEK (inklusive böter). Efter införande av utskriftssäkerhet sjönk det genomsnittliga antalet överträdelser till 1,5, vilket sparade 200 timmar av anställdas arbetstid per år samt 2 miljoner SEK i relaterade kostnader, inklusive revision och efterlevnad.[17]

[16] http://www8.hp.com/us/en/campaign/computersecurity/
[17] IDC The Business Value of Printer Security 2015



Att upptäcka och reagera proaktivt

77 % av IT-säkerhetsutgifterna går till förebyggande och skyddande tekniker som antivirusprogram och brandväggar, enligt forskning av PAC. Men denna strategi är ineffektiv. Forskningen visade också att 67 % av de tillfrågade företagen hade haft ett cyberbrott under de senaste 12 månaderna, och 100 % någon gång i det förflutna.[18]

Speciellt antivirusprogram är chockerande ineffektiva. Damballa genomförde tester där de medvetet attackerade ett nätverk för att mäta antivirusresponsen. Det tog över sex månader innan 100 % av de skadliga filerna hade identifierats.[19] Detta överensstämmer med ett annat konstaterande av PAC att det tog mellan en och sex månader innan företagen upptäckte att de hade attackerats.

Det går inte längre att lita på förebyggande åtgärder för att hålla slutpunkterna säkra. Det ökande antalet incidenter med virus/skadliga programvaror, samt den inbyggda osäkerheten i BYOD/mobilt arbete innebär att överträdelser är oundvikliga. Ingen föreslår att förebyggande och skyddande åtgärder helt ska överges, men att tydligt upptäcka och reagera behöver komma högre upp på dagordningen.

Kontinuerlig övervakning i realtid är nödvändig, helst genom att använda klientenheterna själva som sensorer – och larma resten av nätverket när de har överträtts. Detta gör det möjligt för IT-säkerheten att reagera, inklusive genom processer såsom:

- Via distansstyrning stänga en enhet
- Eliminera en infekterad process, eller en som sprider skadlig programvara
- Lägga en specifik fil eller grupp med filer i karantän
- Avbryta nätverkskommunikationer för att isolera infekterade enheter[20]

Enda sättet att garantera cybersäkerhet, när man inte längre kan förlita sig endast på förebyggande åtgärder, är att acceptera att överträdelser kommer att ske och införa ordentliga responsprotokoller samt den teknik som behövs för att utföra dem.

> “Ingen teknik kan leverera säkerhet om folk underminerar den.”
>
> – Joseph Steinberg [21]

Säkerheten hos de anställda

Att säkra den person som använder en enhet är lika viktig om inte ännu viktigare, än att säkra själva enheten.
Varje anställd måste utbildas i cybersäkerhet. De måste vara medvetna om riskerna med nätfiske, med att surfa på misstänkta webbplatser och ladda ner misstänkta bilagor. De måste vara medvetna om säker lösenordspolicy – använda starka, unika lösenord för varje känslig inloggning och med rätt lösenordshanterare för deras lagring.

De måste bli medvetna om vikten av regelbunden uppdatering av säkerhetsprogram på sin enhet för att minska belastningen på IT-övervakningen. De måste vara uppmärksamma på att ansluta endast säkra enheter till organisationens nätverk och undvika att använda personliga enheter på externa, oskyddade nätverk för att komma åt känsliga data.

Många cybersäkerhetsexperter på hög nivå rekommenderar simuleringar av nätfiskeattacker – de går så långt som att bygga falska nätfiske-webbplatser för att träna alla anställda – och sålunda ta cybersäkerhetsutbildningen till en formell nivå. Eftersom de flesta attacker förlitar sig på att utnyttja den mänskliga svagheten, antingen genom försummelse eller illvilja.

Eftersom människor är den svagaste länken i alla nätverk.

[18] PAC Incident Response Management 2015
[19] https://www.damballa.com/time-to-fix-malware-strategies-2/
[20] The Essential Endpoint Detection Checklist – HP Now
[21] https:// digitalguardian.com/blog/data-security-experts-answer-what-biggest-misconception-companies-have-about-endpoint-security

Slutsats

IT-säkerhetsutgifter bör övergå från att förebygga och skydda till att upptäcka och reagera vid klientenheten.
Skyddandet av en organisations data i det aktuella IT-klimatet – inför ett ökat hot av cyberbrottslighet och en minskad kontroll över nätverkets yttre gränser – kräver två saker: en förändring av själva konceptet och större resurser.

Nätverkskonceptet måste förändras. Idén om nätverket som ett staket runt en samling enheter är inte längre tillämplig. Det är dags att inse verkligheten. ”Nätverket” är en illusion. Det kommer ur anslutna enheter – var för sig en ändpunkt. Att säkra nätverket innebär att säkra ändpunkt. Och varje ändpunkt består av två delar: enheten och den person som använder den. Båda måste beaktas.

Upprätthållandet av säkerheten genom detta nya synsätt är dock betydligt mer komplicerat än vad det var med de enkla stationära datorerna anslutna i en Ethernet-miljö från förr. Det kräver större resurser, och dessa måste prioriteras. Något som 61 % av Ponemons tillfrågade känner igen.

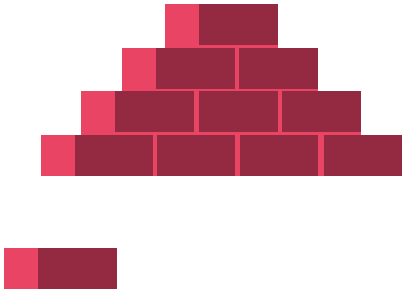
Tricket är att få med resten av organisationen. Endast 36 % av de tillfrågade ansåg att de har gott om budget och personal för klientsäkerhet. 69 % säger att IT-avdelningen inte kan hålla jämna steg med de anställdas efterfrågan på mer stöd. 71 % säger att säkerhetspolicyer för klientenheter är svåra att genomdriva.[22]

80 % av IT-säkerhetscheferna anser regelefterlevnad vara det bästa sättet att motivera finansiering för sina säkerhetsprogram, men de anser också att efterlevnad är den minst viktiga anledningen till spendering. Efterlevnad innebär att uppfylla ett absolut minimum.[23]

IT-beslutsfattare måste samarbeta med ledande befattningshavare för att understryka vikten av säkerhet. Klargör kostnaderna för slapp säkerhet – kostnader för återhämtning, förlorade intäkter, det minskade aktievärdet – och imponera på det långsiktiga sparandet. Många säkerhetslösningar framkallar också förbättringar på andra områden. Tänk på förbättrad produktivitet när man inför utskriftssäkerhet och produktivitetsfördelarna med regelbundet uppdaterad teknik med hjälp av ett flexibelt CYOD-program som erbjuds via en tredje parts abonnemang (som HP DaaS). Uppenbara affärsmässiga förutsättningar kan konstrueras.

Utmaningen är enorm. Och med tiden – med explosionen av enheter i IoT-eran och alltmer sofistikerad cyberbrottslighet – kommer den bara att bli mer problematisk. Men den är inte oövervinnlig. Med rätt teknik, rätt strategi och rätta resurser kan vi försvara våra ändpunkter. Vi kan hålla vår information säker.

Läs mer om HP Device as a Service, och hur det kan hjälpa dig att köra ett omfattande, flexibelt och säkert CYOD-program, **här.**



Registrera dig för uppdateringar på
hp.com/go/getupdated

[22] Ponemon 2016 State of the Endpoint Report
[23] https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697