DRAFT

A Lynchpin Media BRAND

cxo priorities

INTERNA SÄKERHETSHOT – UTMANINGAR OCH PRIORITERINGAR BLAND SVENSKA ORGANISATIONER

I SAMARBETE MED PROOFPOINT

proofpoint.

proofpoint.

priorities

A Lynchpin Media BRAND

INNEHÅLL

proofpoint

priorities

A Lynchpin Media BRAND

INLEDNING

Säkerhetsmedvetande har blivit en allt viktigare fråga för organisationer under de senaste åren, särskilt i och med införandet av hybridarbete och ökade interna hot.

Trots försök att förstärka IT-säkerheten uppstår dagligen nya utmaningar som ofta kan leda till dataintrång eller förlust av känslig information.

Angriparna är alltför medvetna om brister i säkerheten och hittar sätt att utnyttja dem, med stöld av inloggningsuppgifter och varumärkesskador som följd.

Allt eftersom det blivit lättare för medarbetare att läcka data utanför säkerhetsinfrastrukturen har det blivit mer utmanande för organisationer att förbättra säkerheten i hela verksamheten.

Det krävs att organisationen förstår sig på den nuvarande hotbilden från interna hot och prioriterar införandet av en robust säkerhet för att förhindra dataintrång och skydda känsliga data.

För att lära oss mer om säkerhetstänket och medarbetarträning inom säkerhetsmedvetenhet skickade vi ut en enkät till 75 chefer i svenska företag. Sammanlagt 36% av deltagarna hörde till offentliga organisationer medan de resterande 64% var verksamma inom den privata sektorn.

MED DEN HÄR UNDERSÖKNINGEN VILLE VI FÅ REDA PÅ:

- Hur organisationer prioriterar säkerheten och förbättrar säkerhetsmedvetandet bland sina medarbetare
- Hur ofta dataintrång sker i deras organisationer, varför de sker och vad de leder till
- Vilka rutiner som finns för att skydda mot interna hot
- Vilka utmaningar organisationen ställs inför som ökar risker med interna hot

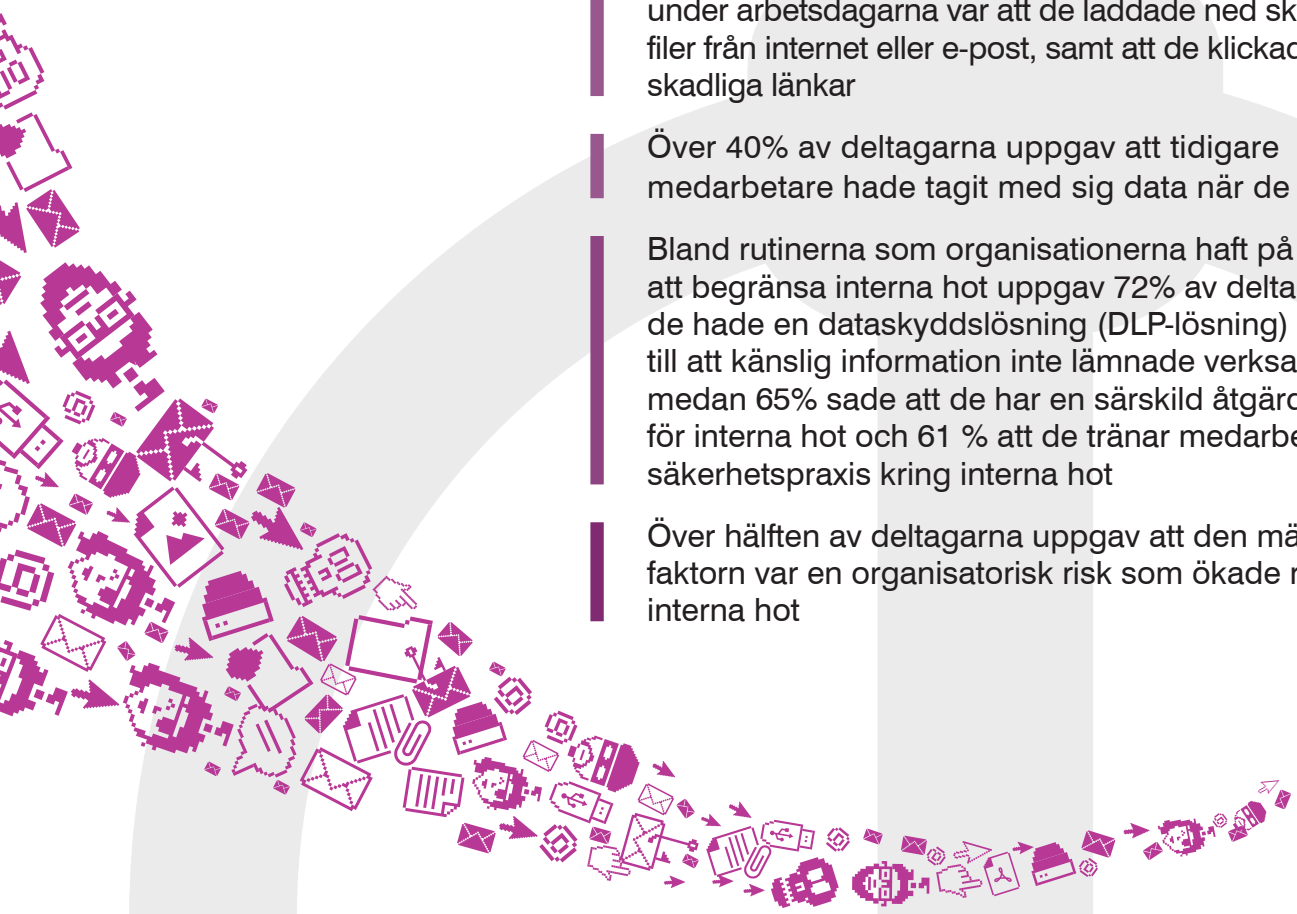
proofpoint.

priorities

A Lynchpin Media BRAND

SAMMANFATTNING AV RESULTATEN:

- Närmare 50% av deltagarna i undersökningen hade drabbats av ett dataintrång eller förlust av känslig information under de senaste 12 månaderna
- Stöld av inloggningsuppgifter är den främsta orsaken till dataintrång, följt av borttappade/stulna enheter
- Över 50% av deltagarna uppgav att interna hot är en viktig cybersäkerhetsfråga för dem under de kommande två åren
- Att medarbetare lättare kan läcka data utanför kontorets säkerhetsinfrastruktur, samt att man saknar insyn i vad medarbetarna gör, uppgavs vara de två största riskerna som uppstått på grund av hybridarbete
- Det vanligaste beteendet som medarbetare uppvisade under arbetsdagarna var att de laddade ned skadliga filer från internet eller e-post, samt att de klickade på skadliga länkar
- Över 40% av deltagarna uppgav att tidigare medarbetare hade tagit med sig data när de slutat
- Bland rutinerna som organisationerna haft på plats för att begränsa interna hot uppgav 72% av deltagarna att de hade en dataskyddslösning (DLP-lösning) för att se till att känslig information inte lämnade verksamheten, medan 65% sade att de har en särskild åtgärdsplan för interna hot och 61 % att de tränar medarbetare i säkerhetspraxis kring interna hot
- Över hälften av deltagarna uppgav att den mänskliga faktorn var en organisatorisk risk som ökade risken för interna hot



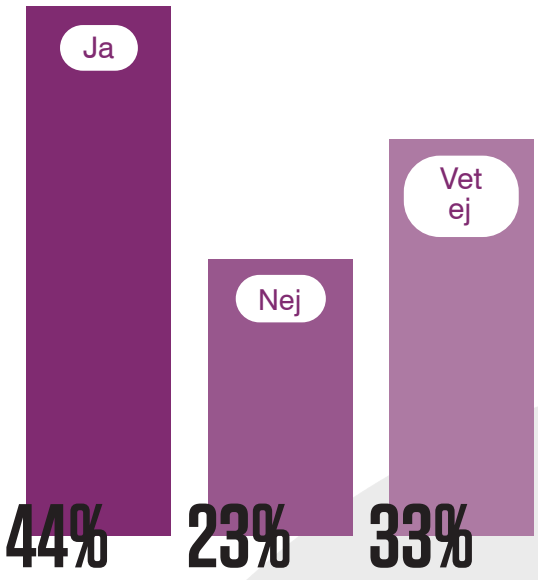
proofpoint

priorities

A Lynchpin Media BRAND

AVSNITT 01: UTMANINGARNA OCH HOTBILDEN

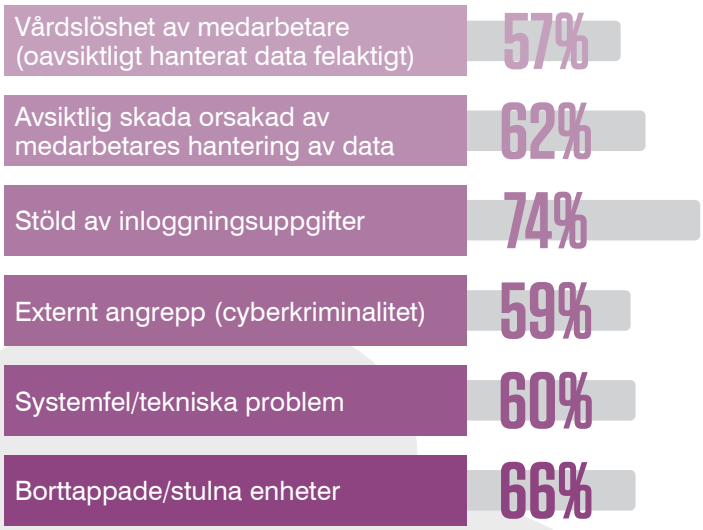
Har er organisation drabbats av ett dataintrång/förlust av känslig information under de senaste 12 månaderna?



SAMMANFATTNING

Närmare 50 % av deltagarna uppgav att deras organisation drabbats av ett dataintrång eller förlust av känslig information under de senaste 12 månaderna, vilket pekar på ett behov att stärka verksamhetens säkerhet.

Vad var orsaken till dataintrånget? (Kryssa i alla alternativ som stämmer)



SAMMANFATTNING

Nästan tre fjärdedelar (74%) av alla deltagare i undersökningen ansåg att stulna inloggningsuppgifter var den största orsaken till dataintrång, strax därefter följt av borttappade/stulna enheter (66%) och avsiktlig skada eller stöld från medarbetare (62%). Detta pekar på ett behov att förstärka säkerhetsmedvetandet och främja ett säkerhetstänk som gör medarbetare uppmärksamma på cyberattacker.

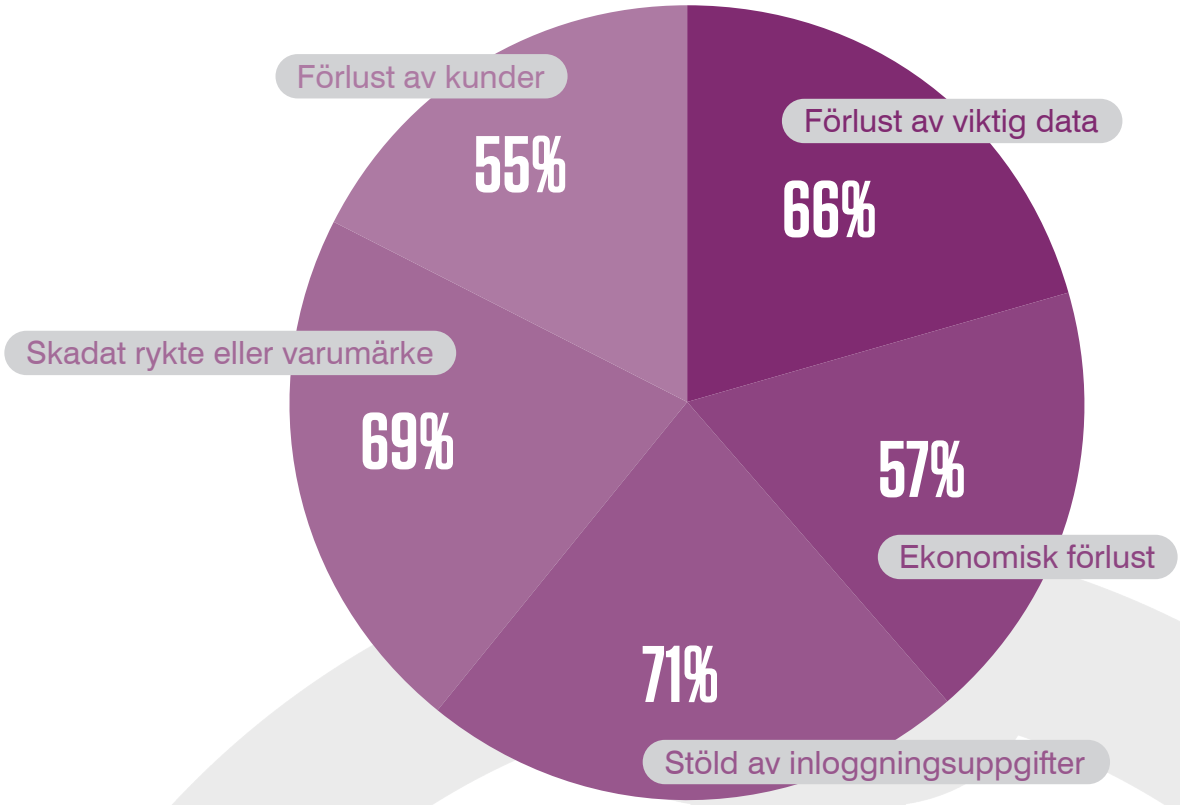
proofpoint

priorities

A Lynchpin Media BRAND

AVSNITT 01: UTMANINGARNA OCH HOTBILDEN FORTSATT...

Vad blev den slutgiltiga följden av intrånget i er organisation? (Kryssa i alla alternativ som stämmer)



SAMMANFATTNING

Alla dessa orsaker kan få katastrofala följder för verksamheten. Resultaten visar att stöld av inloggningsuppgifter (71%) var den vanligaste följden av ett dataintrång, strax därefter följt av skadat rykte eller varumärke (69%) samt förlust av viktig data (66%).

proofpoint

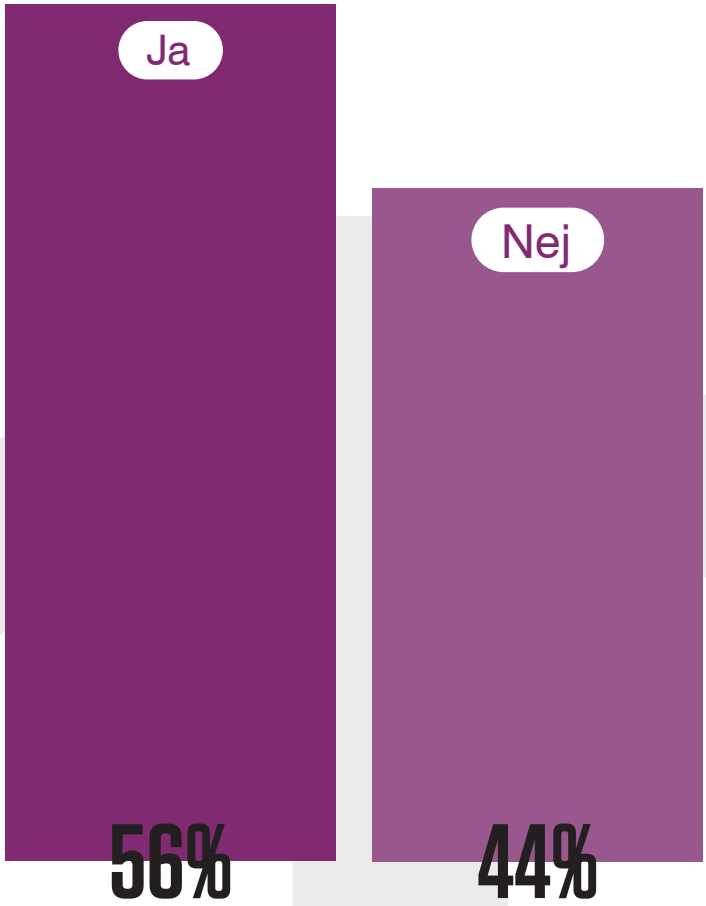
priorities

A Lynchpin Media BRAND

AVSNITT 2: PRIORITERINGAR OCH UTSIKTERNA FRAMÖVER

Bland det viktigaste för att skapa en robust säkerhet är att främja säkerhetsmedvetandet. Hybridarbete ställer också krav på cybersäkerhetsträning av en hög kaliber med tanke på hur mycket lättare det blivit att medarbetare läcker data utanför verksamhetens säkerhetsinfrastruktur.

Är interna hot en viktig cybersäkerhetsfråga för er under de kommande två åren?



SAMMANFATTNING

Över hälften (56%) av deltagarna uppgav att interna hot kommer att vara en central cybersäkerhetsfråga under de kommande två åren. Detta påvisar uppfattningen om hotbilden och belyser också behovet att ge säkerhetsteam tillräckliga befogenheter samt att förstärka åtgärderna kring interna hot.

proofpoint.

priorities

A Lynchpin Media BRAND

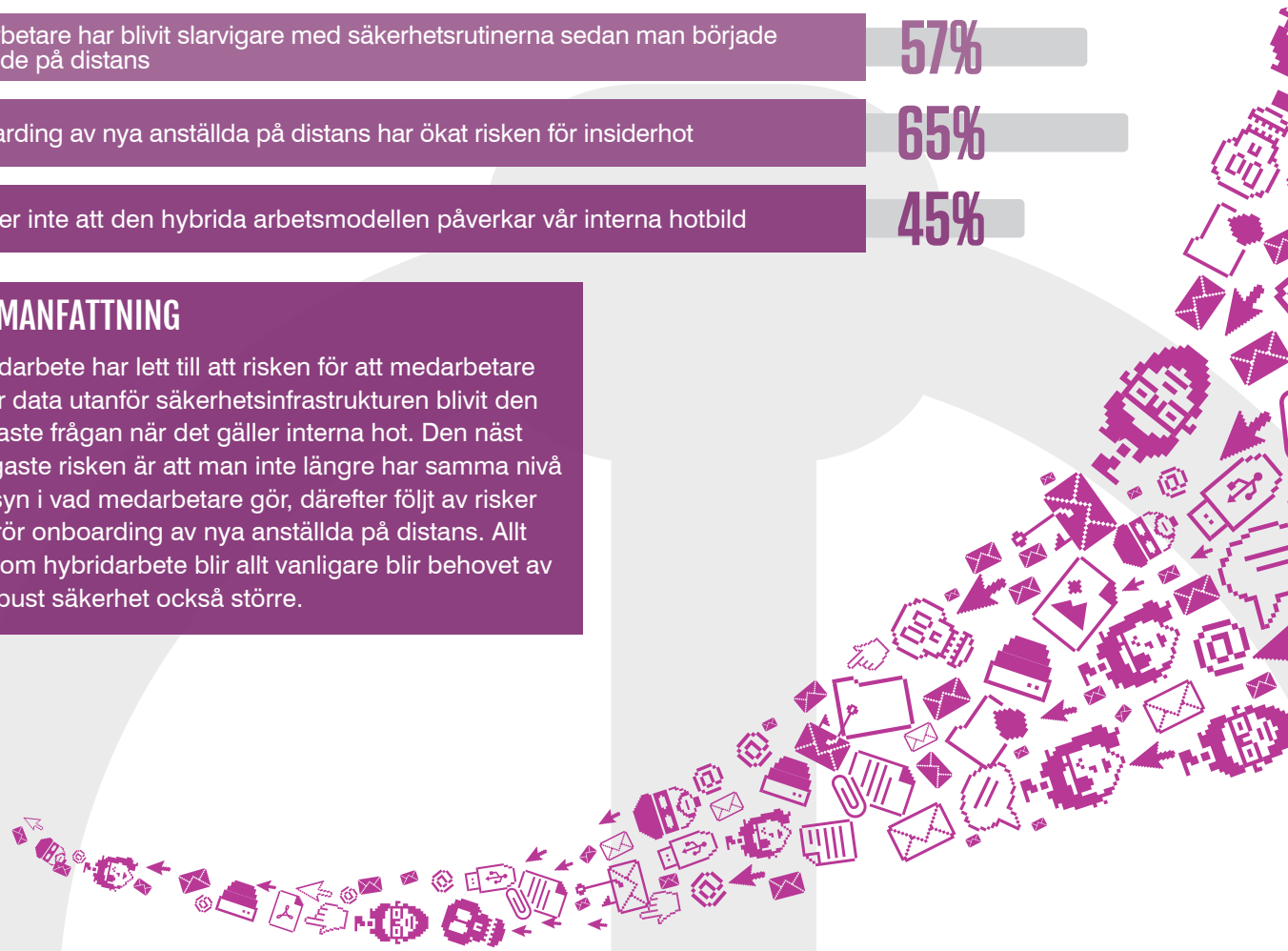
AVSNITT 2: PRIORITERINGAR OCH UTSIKTERNA FRAMÖVER FORTSATT...

Vilka av följande påståenden håller du med om ifråga om interna hot på grund av hybridarbete? (Kryssa i alla alternativ som stämmer)

Ökad användning av samarbetsplattformar i molnet innebär att vi är mer utsatta för risker	57%
Det är lättare för medarbetare att läcka data utanför kontorets säkerhetsinfrastruktur	69%
Vi har inte samma nivå av insyn i vad våra medarbetare gör	68%
Medarbetare har blivit slarvigare med säkerhetsrutinerna sedan man började arbetade på distans	57%
Onboarding av nya anställda på distans har ökat risken för insiderhot	65%
Vi anser inte att den hybrida arbetsmodellen påverkar vår interna hotbild	45%

SAMMANFATTNING

Hybridarbete har lett till att risken för att medarbetare läcker data utanför säkerhetsinfrastrukturen blivit den viktigaste frågan när det gäller interna hot. Den näst vanligaste risken är att man inte längre har samma nivå av insyn i vad medarbetare gör, därefter följt av risker som rör onboarding av nya anställda på distans. Allt eftersom hybridarbete blir allt vanligare blir behovet av en robust säkerhet också större.



proofpoint

priorities

A Lynchpin Media BRAND

AVSNITT 2: PRIORITERINGAR OCH UTSIKTERNA FRAMÖVER FORTSATT...

Har era medarbetare uppvisat något av följande beteende under arbetsdagen? (Kryssa i alla alternativ som stämmer)

56%

Använder USB-stickor

67%

Klickar på skadliga länkar

65%

Delar företagets enheter med familj/vänner

67%

Laddar ned skadliga filer från internet eller e-post

61%

Delar med sig av inloggningsuppgifter av misstag

57%

Ansluter till osäkra Wi-Fi

0%

Delar företagsinformation med extern angripare/aktör

SAMMANFATTNING

Det vanligaste beteendet som medarbetare uppvisade under arbetsdagarna var att de laddade ned skadliga filer från internet eller e-post, samt att de klickade på skadliga länkar. Näst vanligast var, enligt deltagarna i undersökningen, att medarbetare delade organisationens enheter med familj och vänner. Detta belyser behovet av att träna medarbetare i säkerhetsmedvetande.

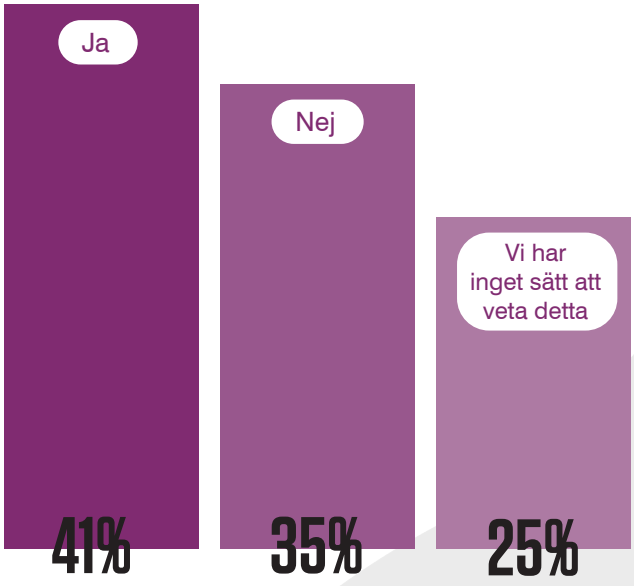
proofpoint

CXO priorities

A Lynchpin Media BRAND

AVSNITT 2: PRIORITERINGAR OCH UTSIKTERNA FRAMÖVER FORTSATT...

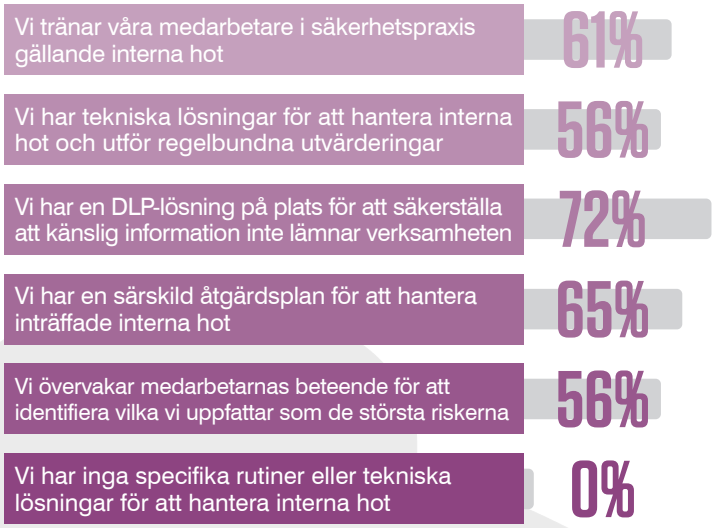
Har det skett att en tidigare medarbetare i er organisation tagit med sig data när de slutat?



SAMMANFATTNING

Medan 41% av deltagarna uppgav att tidigare medarbetare hade tagit med sig data när de slutat, uppgav 25% att de inte hade något sätt att veta om det hade skett. Detta påvisar att det fortfarande finns en del utrymme för förbättring i främjandet och etablerandet av en säkerhetskultur.

Vilka rutiner har ni på plats för att förebygga interna hot? (Kryssa i alla alternativ som stämmer)



SAMMANFATTNING

En etablerad DLP-lösning som säkerställer att känslig information inte lämnar verksamheten (72%) är viktigast för att motverka interna hot. Detta följs av en särskild åtgärdsplan för inträffade interna hot (65%) och utbildning av medarbetare i säkerhetspraxis kring interna hot (61%). Med tanke på hur dessa hot fungerar så tyder det på behov att investera mer i medarbetarnas säkerhetsmedetande.

proofpoint

priorities

A Lynchpin Media BRAND

AVSNITT 2: PRIORITERINGAR OCH UTSIKTERNA FRAMÖVER FORTSATT...

Vilka frågor tog ni upp i organisationens medarbetarträning i cybersäkerhetsmedvetande? (Kryssa i alla alternativ som stämmer)

59%
E-post-baserade hot (nätfiske, kapade eller förfalskade e-postadresser)

59%
Dataskydd

64%
Molnbaserad säkerhet

57%
Säkerhet kring Wi-Fi

61%
Utpressningsprogram

64%
Lösenordshygien

49%
Säkerhetspraxis i användningen av organsationens eller egna enheter

0% Interna hot

0% Vi har inget pågående träningsprogram för cybersäkerhetsmedvetenhet

SAMMANFATTNING

De vanligaste frågorna som tagits upp under medarbetarnas träning i cybersäkerhet var interna hot (64%) och lösenordshygien (64%), strax därefter följt av utpressningsprogram (61%).

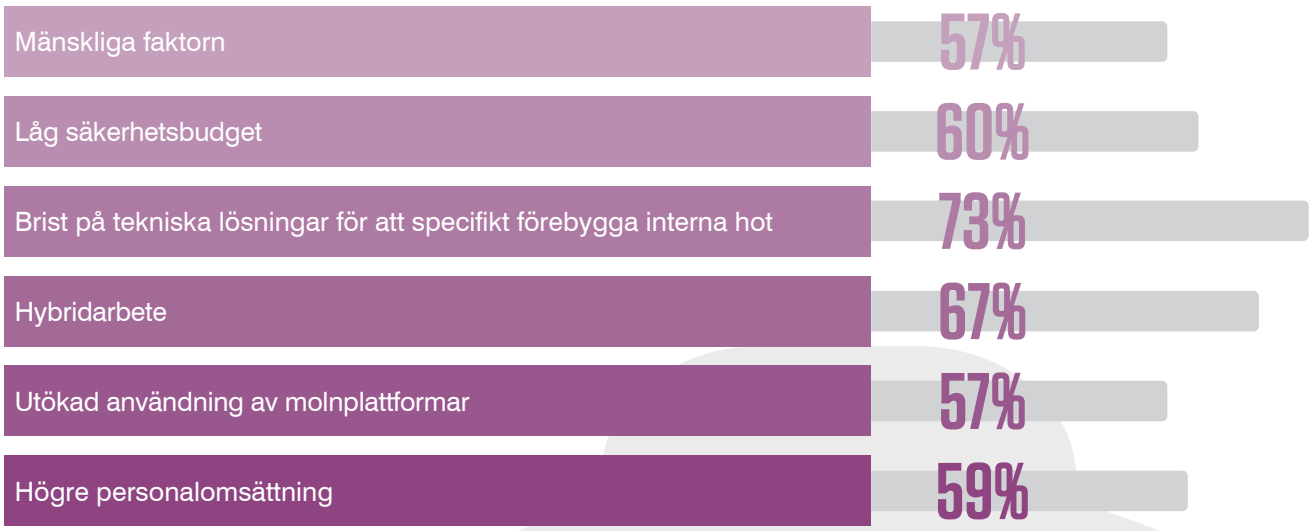
proofpoint.

priorities

A Lynchpin Media BRAND

AVSNITT 2: PRIORITERINGAR OCH UTSIKTERNA FRAMÖVER FORTSATT...

Vilka organisatoriska utmaningar tror du ökar er risk att utsättas för interna hot? (Kryssa i alla alternativ som stämmer)



SAMMANFATTNING

Sammanlagt 73% av deltagarna ansåg att bristen på tekniska lösningar specifikt för interna hot var verksamhetens största utmaning som ökar risken för interna hot, medan 67% ansåg att hybridarbete var den näst största utmaningen. Detta belyser behovet av att förstärka infrastruktursäkerheten, utöver att erbjuda medarbetarna träning. Även begränsade säkerhetsbudgetar (60%) ansågs vara en utmaning som bidrog till risken för interna hot, vilket pekar på behovet av ökad investering i säkerhet.

proofpoint.

priorities

A Lynchpin Media BRAND

SLUTSATSER

> IMPLEMENTERA EN STRATEGI FÖR ATT FÖRÄNDRA SÄKERHETSBETEENDET OCH FRÄMJA EN SÄKERHETSKULTUR INOM VERKSAMHETEN, OCH FÖR ATT BIDRA TILL ATT BEGRÄNSA HUR OFTA MEDARBETARE KLICKAR PÅ SKADLIGA LÄNKAR, FALLER FÖR NÄTFISKE, LADDAR NED OSÄKRA FILER, ELLER DELAR VERKSAMHETENS ENHETER, SAMT FÖR ATT TA UPP VIKTEN AV ATT HÅLLA ORGANISATIONENS UPPGIFTER SÄKRA.

Då majoriteten av deltagarna uppger att deras organisation drabbats av ett dataintrång eller en förlust av känslig information under det senaste året är det hög tid att investera i träning i säkerhetsmedvetande och att utveckla ett robust säkerhetstänk.

Det föreligger ett tydligt behov att träna medarbetare i säkerhetsmedvetande eftersom stulna inloggningsuppgifter, samt stulna eller borttappade enheter, är den främsta orsaken till dataintrång.

56% av deltagarna uppgav att interna hot var en central fråga för cybersäkerheten inom de kommande två åren, vilket innebär att det är av högsta vikt att organisationer blickar framåt och fokuserar på långsiktiga strategier inom säkerhetsmedvetande och cybersäkerhet.

Risken för interna hot i form av att medarbetare lättare kan läcka data har ökat i och med införandet av hybridarbete. Medarbetare har en tendens att ladda ned skadliga filer från internet eller e-post och delar ofta organisationens enheter med familjemedlemmar.

Organisationerna behöver göra ytterligare investeringar i tekniska lösningar som specifikt handskas med interna hot samt utöka sina medarbetares kunskap om dessa och hur man kan undvika att de inträffar av misstag.

En långsiktig approach med hjälp av en stark partner behövs för att stödja främjandet och förstärkningen av en säkerhetskultur som ökar säkerhetsmedvetandet och i förlängningen begränsar risken från interna hot.

proofpoint.

priorities

A Lynchpin Media BRAND

Sponsored by
proofpoint.

c/o iOffice
Kungsgatan 37, 8 tr
111 56 Stockholm

Find out more:
www.proofpoint.com/uk

priorities

CxO Priorities, a Lynchpin Media Brand
63/66 Hatton Garden
London, EC1N 8LE

Find out more:
www.cxopriorities.com