A Lynchpin Media BRAND

cxo priorities

HET RISICOLANDSCHAP VAN INTERNE DREIGINGEN – UITDAGINGEN EN PRIORITEITEN VOOR NEDERLANDSE ORGANISATIES

IN SAMENWERKING MET PROOFPOINT

proofpoint.

proofpoint.

priorities

A Lynchpin Media BRAND

INHOUD

proofpoint.

priorities

A Lynchpin Media BRAND

INTRODUCTIETEKST

Met de wereldwijde adoptie van een hybride werkcultuur hebben organisaties een toename van interne dreigingen waargenomen. Hierdoor wordt er nu meer waarde gehecht aan beveiligingsbewustzijn, het creëren van een beveiligingscultuur waarin werknemers beter voorbereid zijn op zulke dreigingen.

Organisaties worden dagelijks geconfronteerd met nieuwe beveiligingsuitdagingen en de afwezigheid van een sterke beveiligingscultuur kan aanvallers in de kaart spelen, met de consequenties van een succesvolle aanval als gevolg. Dit kan leiden tot het verlies van gegevens of gevoelige informatie, diefstal van inloggegevens, reputatieschade en verloren klanten.

Aangezien interne dreigingen een zeer belangrijk punt van zorg aan het worden zijn voor organisaties, is het van cruciaal belang om te investeren in training voor beveiligingsbewustzijn en werknemers van de benodigde tools te voorzien.

We hebben een enquête gehouden onder 75 hogere leidinggevenden om beter te begrijpen wat de interne dreiging is en wat hun benadering is ten opzichte van beveiligingscultuur en bewustzijnstraining. In totaal kwam 29% van de ondervraagden uit publieke organisaties en de overige 71% uit private organisaties.

MET DEZE ENQUÊTE WILDEN WE HET VOLGENDE ONTDEKKEN:

- Hoe organisaties het beveiligingsbewustzijn van hun medewerkers kunnen verbeteren;
- Hoe frequent datalekken voorkomen en hoeveel van de ondervraagden interne dreigingen als een toekomstig risico beschouwen;
- De protocollen die organisaties hebben om interne dreigingen te voorkomen;
- De prioriteiten met betrekking tot training voor bewustzijn op het gebied van cybersecurity.

proofpoint.

priorities

A Lynchpin Media BRAND

SAMENVATTING VAN DE RESULTATEN:

- Bijna 50% van de ondervraagden heeft in de afgelopen 12 maanden te maken gehad met een datalek of verlies van gevoelige informatie met diefstal van inloggegevens en reputatieschade tot gevolg;
- Bijna 50% van de ondervraagden gaf aan dat zij interne dreiging beschouwen als een belangrijk cybersecurity-probleem voor henzelf in de komende twee jaar;
- 'Hetzelfde niveau van inzicht hebben in wat werknemers doen' en 'het onboarden van nieuwe werknemers op afstand' werden beschouwd als de twee belangrijkste risico's met betrekking tot interne dreiging, veroorzaakt door hybride werken;
- 'Het delen van apparaten met familie of vrienden' en 'het per ongeluk delen van accountgegevens' waren twee van de belangrijkste gedragingen waaraan werknemers zich gedurende de werkdag schuldig maakten;
- In totaal gaf 40% van de ondervraagden aan dat werknemers hun bedrijf hadden verlaten en gegevens hadden meegenomen;
- Van de protocollen die organisaties hebben opgesteld om interne dreigingen te voorkomen, heeft 68% van de ondervraagden een DLP-toepassing (Data Loss Prevention) om te voorkomen dat gevoelige informatie het bedrijf verlaat, terwijl 63% aangaf dat zij werknemers trainen in aanbevolen procedures voor beveiliging met betrekking tot interne dreiging;
- Meer dan de helft van de ondervraagden gaf aan dat menselijke fouten een organisatorisch risico vormden die het gevaar van interne dreigingen verhoogde, terwijl het gebrek aan specifieke technologie voor interne dreiging als hoogste werd gekozen door 77%.

proofpoint

priorities

A Lynchpin Media BRAND

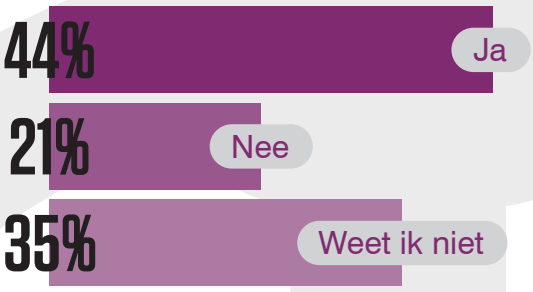
HOOFDSTUK 1: DE UITDAGINGEN EN HET DREIGINGSLANDSCHAP

Bewustzijn en training omtrent beveiliging zijn al een paar jaar een prioriteit voor veel organisaties. Met de toename van interne dreiging en de adoptie van een hybride werkcultuur is de noodzaak voor het verbeteren van training en het opzetten van een sterke beveiligingscultuur echter nog belangrijker geworden.

Omdat de gevolgen van een interne dreiging desastreus kunnen zijn, moeten organisaties hun werknemers van kennis voorzien en ze voorbereiden met de juiste benaderingen voor zowel preventie als reactie.

In dit hoofdstuk verkennen we hoe gangbaar datalekken zijn bij organisaties, wat de meest voorkomende oorzaken zijn en welk effect ze hebben.

Heeft uw organisatie in de afgelopen 12 maanden last gehad van een datalek of verlies van gevoelige informatie?



BELANGRIJKSTE BEVINDING

Bijna 50% van de deelnemers gaf aan dat hun organisatie in het voorafgaande jaar last heeft gehad van een datalek of verlies van gevoelige informatie. Er bestaat een duidelijke noodzaak om beveiligingsmaatregelen te verbeteren en een stevige beveiligingscultuur op te zetten.

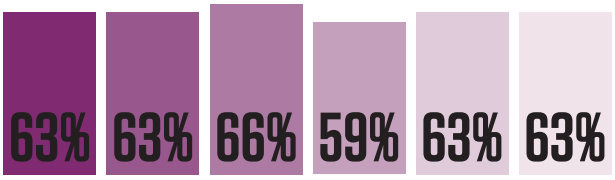
proofpoint

priorities

A Lynchpin Media BRAND

HOOFDSTUK 1: DE UITDAGINGEN EN HET DREIGINGSLANDSCHAP VOORTGEZET...

Wat was de oorzaak van het datalek? (Vink alles aan dat van toepassing is) (Percentage ondervraagden dat de desbetreffende optie heeft geselecteerd)

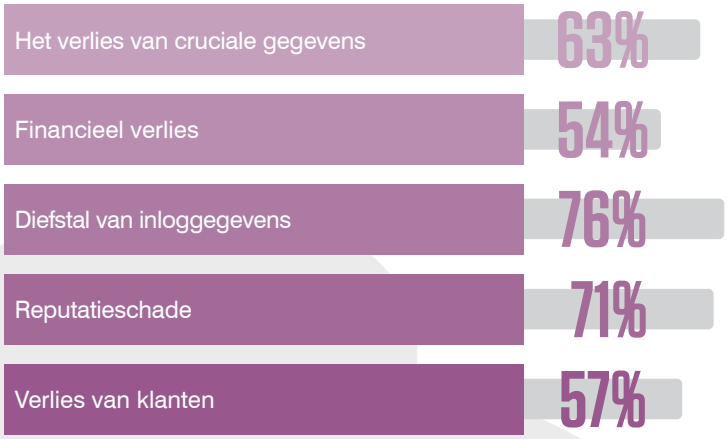


- Nalatige werknemer/onvoorzichtigheid van werknemer (Een werknemer die onbewust gegevens misbruikt)
- Kwaadaardige of criminele werknemer (Een werknemer die gegevens misbruikt met als doel het opzettelijk schaden van de organisatie)
- Diefstal van inloggegevens
- Externe aanval (cybercrimineel)
- Systeem-/technische problemen
- Verloren/gestolen apparaten

BELANGRIJKSTE BEVINDING

Elk van deze uitkomsten kan negatieve effecten hebben voor het functioneren van een organisatie. Volgens de ondervraagden is het meest voorkomende eindresultaat van de inbreuk op hun organisatie de diefstal van inloggegevens (76%), gevolgd door reputatieschade (71%) en verlies van cruciale gegevens (63%), waarbij de noodzaak voor een sterkere strategie voor beveiligingsbewustzijn wordt aangehaald.

Wat was het uiteindelijke resultaat van de inbreuk op uw organisatie? (Vink alles aan dat van toepassing is) (Percentage ondervraagden dat de desbetreffende optie heeft geselecteerd)



BELANGRIJKSTE BEVINDING

Elk van deze uitkomsten kan negatieve effecten hebben voor het functioneren van een organisatie. Volgens de ondervraagden is het meest voorkomende eindresultaat van de inbreuk op hun organisatie de diefstal van inloggegevens (76%), gevolgd door reputatieschade (71%) en verlies van cruciale gegevens (63%), waarbij de noodzaak voor een sterkere strategie voor beveiligingsbewustzijn wordt aangehaald.

proofpoint

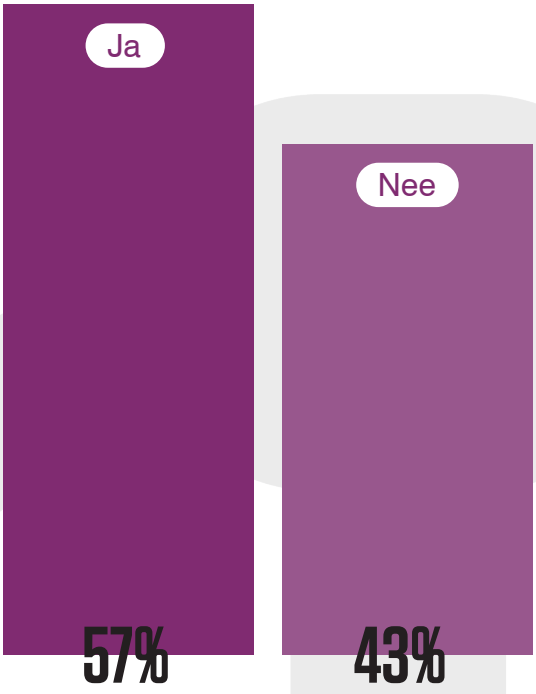
priorities

A Lynchpin Media BRAND

HOOFDSTUK 2: PRIORITEITEN EN VOORUITZICHTEN

Aangezien interne dreigingen een steeds belangrijkere bron van zorg aan het worden zijn, moeten organisaties meer investeren in het scholen van hun werknemers. Daarnaast bestaat er behoefte aan een geschikt reactieplan, gezien het gemak waarmee werknemers door het hybride werken bedrijfsgegevens kunnen delen buiten de grenzen van de beveiligingsinfrastructuur.

Zijn interne dreigingen een belangrijk cybersecurity-probleem voor u in de komende twee jaar?



BELANGRIJKSTE BEVINDING

Meer dan 50% van de ondervraagden beschouwt interne dreigingen als een zeer belangrijk cybersecurity-probleem voor de komende twee jaar. De ondervraagden zien interne dreigingen als significant. Daarnaast moeten werknemers worden getraind in het reageren op interne dreigingen, zodat ze goed voorbereid zijn in het geval dat er een datalek plaatsvindt.

proofpoint.

priorities

A Lynchpin Media BRAND

HOOFDSTUK 2: PRIORITEITEN EN VOORUITZICHTEN VOORTGEZET...

Met welke van de volgende uitspraken bent u het eens als het gaat om het risico van interne dreiging veroorzaakt door hybride werken? (Vink alles aan dat van toepassing is) (Percentage ondervraagden dat de desbetreffende optie heeft geselecteerd)

Het toenemende gebruik van cloudsamenwerkingsplatforms maakt ons kwetsbaarder voor dreigingen	59%
Werknemers kunnen gemakkelijker data lekken buiten de grenzen van de beveiligingsinfrastructuur op kantoor	56%
We hebben niet hetzelfde niveau van inzicht in wat onze werknemers doen	76%
Werknemers zijn lakser geworden met beveiligingsprocedures sinds zij op afstand zijn gaan werken	56%
Het onboarden van nieuwe werknemers op afstand heeft de risico's van interne dreigingen verhoogd	73%
We denken niet dat het hybride werkmodel ons risico van interne dreigingen verhoogt	43%

BELANGRIJKSTE BEVINDING

Meer dan een derde van de ondervraagden gelooft dat het ontbreken van hetzelfde niveau van inzicht in wat werknemers doen de belangrijkste interne dreiging is als gevolg van hybride werk, op de voet gevolgd door het onboarden van nieuwe werknemers op afstand. Daarnaast is 50% van de ondervraagden ook bezorgd over het gemak waarmee werknemers gegevens kunnen lekken buiten de grenzen van de beveiligingsinfrastructuur op het kantoor. Aangezien hybride werken nu wereldwijd geaccepteerd is, moet er een sterkere beveiligingscultuur voor de organisatie worden gecreëerd.

proofpoint

priorities

A Lynchpin Media BRAND

HOOFDSTUK 2: PRIORITEITEN EN VOORUITZICHTEN VOORTGEZET...

Hebben of vertonen uw werknemers één of meer van de onderstaande gedragingen tijdens hun werkdag? (Vink alles aan dat van toepassing is)

55%

Gebruik van USB-stations

56%

Klikken op kwaadaardige URL-koppelingen

76%

Delen van apparaten met familie of vrienden

59%

Downloaden van kwaadaardige bijlagen of bestanden

60%

Per ongeluk delen van accountgegevens

56%

Verbinden met onveilige wifinetwerken

0%

Delen van bedrijfsinformatie met een externe aanvaller of bron

BELANGRIJKSTE BEVINDING

Meer dan een derde van de ondervraagden gelooft dat het delen van apparaten met familie en vrienden de meest voorkomende gedraging is waaraan werknemers zich gedurende werkdag schuldig maken. De op één na meest voorkomende gedraging is het per ongeluk delen van inloggegevens, gevolgd door het downloaden van kwaadaardige bijlagen en bestanden.

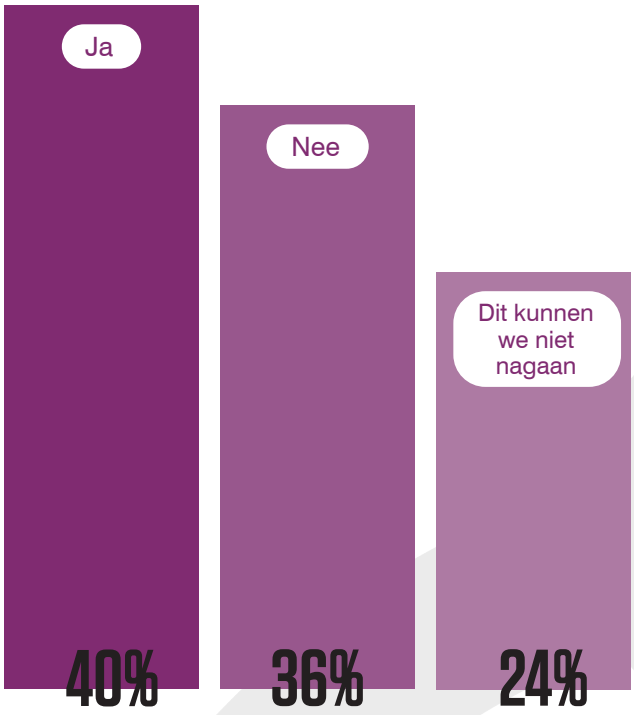
proofpoint.

CXO priorities

A Lynchpin Media BRAND

HOOFDSTUK 2: PRIORITEITEN EN VOORUITZICHTEN VOORTGEZET...

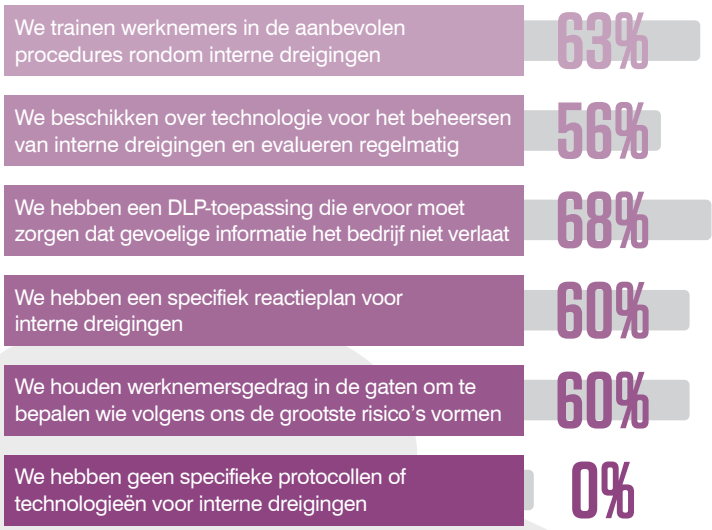
Heeft u werknemers gehad die uw organisatie hebben verlaten en gegevens hebben meegenomen?



BELANGRIJKSTE BEVINDING

Terwijl 40% van de ondervraagden aangaf dat werknemers hun organisatie hadden verlaten en gegevens hadden meegenomen, kon 24% dat niet nagaan. Dit laat zien dat er ruimte is voor een betere benadering van het weten waar gegevens zich op elk moment begeven en voor het implementeren van strenger beleid om te voorkomen dat werknemers gegevens kunnen meenemen.

Welke protocollen heeft u om interne dreigingen te voorkomen? (Vink alles aan dat van toepassing is)



BELANGRIJKSTE BEVINDING

Als het gaat om protocollen die tot doel hebben om interne dreigingen te voorkomen, is de meest populaire een DLP-toepassing die ervoor moet zorgen dat gevoelige informatie het bedrijf niet verlaat (68%). Dit wordt gevolgd door het trainen van werknemers in de beste aanbevolen procedure rondom interne dreigingen (63%). Daarnaast is er een reactieplan voor de risico's van werknemers (60%) en het in de gaten houden van het gedrag van werknemers om de grootste risico's te identificeren. Dit geeft aan hoe organisaties de samenwerking tussen technologie en training zien.

proofpoint.

priorities

A Lynchpin Media BRAND

HOOFDSTUK 2: PRIORITEITEN EN VOORUITZICHTEN VOORTGEZET...

Welke onderwerpen komen aan bod in uw organisatorische bewustzijnstraining voor het cybersecurity? (Vink alles aan dat van toepassing is)

56%

Bedreigingen via e-mail (phishing, compromittering van zakelijke e-mail)

60%

Gegevensbeveiliging

53%

Interne dreigingen

64%

Cloud-gebaseerde beveiliging

51%

Beveiliging wifinetwerk

61%

Ransomware

55%

Verantwoord wachtwoordgebruik

57%

Aanbevolen procedures voor het gebruik van zakelijke en persoonlijke apparaten

0%

We hebben momenteel geen programma voor cybersecurity-bewustzijn

BELANGRIJKSTE BEVINDING

De meest populaire onderwerpen als het gaat om organisatorische cybersecurity-bewustzijn zijn: cloud-gebaseerde beveiliging (64%), gevolgd door ransomware (61%) en gegevensbeveiliging (60%).

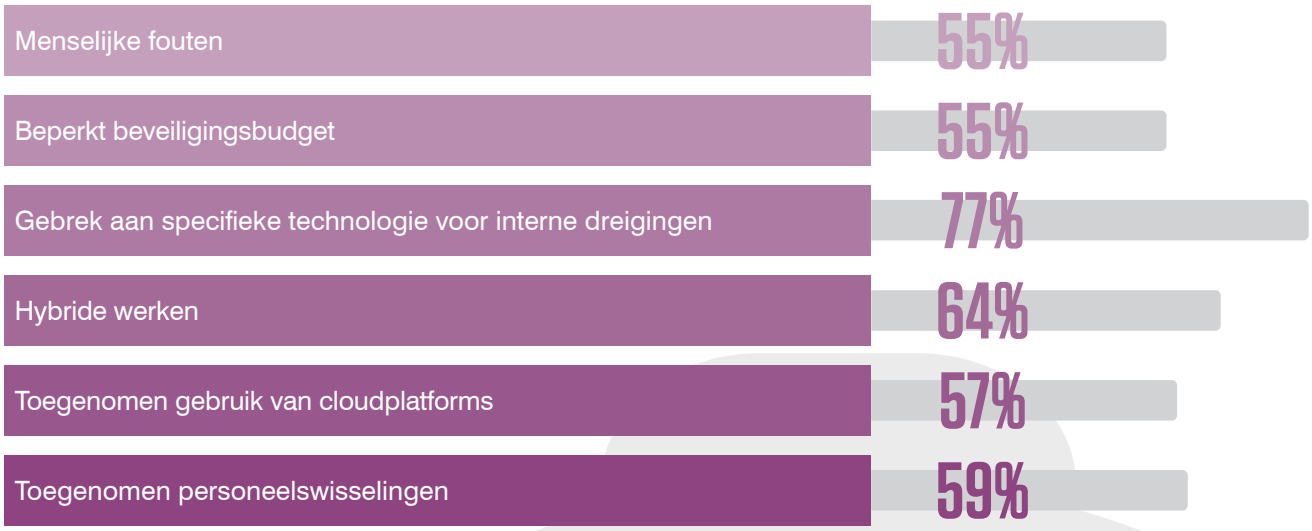
proofpoint.

CXO priorities

A Lynchpin Media BRAND

HOOFDSTUK 2: PRIORITEITEN EN VOORUITZICHTEN VOORTGEZET...

Welke organisatorische uitdagingen denkt u dat uw risico op interne dreigingen verhogen? (Vink alles aan dat van toepassing is)



BELANGRIJKSTE BEVINDING

Meer dan een derde van de ondervraagden is van mening dat een gebrek aan specifieke technologie voor interne dreigingen hun risico verhoogt. Dit wordt gevolgd door de organisatorische dreiging van hybride werken en toegenomen personeelswisselingen. Hierdoor is het noodzakelijk de beveiligingscultuur van de organisatie te verbeteren en het beveiligingsbewustzijn van de organisatie te trainen.

proofpoint.

CXO priorities

A Lynchpin Media BRAND

CONCLUSIE

Gezien bijna de helft van de ondervraagden aangeeft dat hun organisatie hinder heeft ondervonden van een datalek of verlies van gevoelige informatie, is het duidelijk dat training omtrent beveiligingsbewustzijn noodzakelijk is, vooral omdat diefstal van inloggegevens de meest voorkomende oorzaak is van datalekken.

Daarnaast kunnen diefstal van inloggegevens en reputatieschade als gevolg van het verlies van gevoelige informatie desastreuze gevolgen hebben voor de organisatie. Het is cruciaal voor organisaties om zich voor te bereiden op de toekomst en langetermijnstrategieën te ontwikkelen die bijdragen aan een efficiënte beveiligingscultuur.

> VOER EEN RISICOANALYSE UIT VOOR DE GEBRUIKTE CLOUDDIENSTEN OM DE HUIDIGE POSITIE VAN UW ORGANISATIE MET BETREKKING TOT HET IDENTIFICEREN VAN VERDACHTE TOEGANG, HET ONRECHTMATIG DELEN VAN GEGEVENS EN RISKANT GEBRUIK VAN CLOUDAPPLICATIES VAST TE STELLEN.

Aangezien het delen van apparaten met familie en vrienden standaardgedrag is dat werknemers vertonen, moeten zij worden getraind en worden voorzien van de juiste tools voor het ontwikkelen van beveiligingsbewustzijn.

Met de adoptie van de hybride werkcultuur is het risico van interne dreigingen toegenomen. Als gevolg hiervan moeten organisaties hun werknemers trainen om onbedoeld verlies van gegevens te voorkomen en om ze uit te rusten met een effectief reactieplan.

Door een langetermijnbenadering te volgen en zich van een betrouwbare partner te verzekeren kunnen CISO's een veel sterkere beveiligingscultuur opzetten en hun werknemers beveiligingsbewustzijn bijbrengen, wat uiteindelijk de risico's die cyberbedreigingen vormen helpt te verminderen.

proofpoint.

priorities

A Lynchpin Media BRAND

Sponsored by
proofpoint.

Cyber House, Unit 11 Weavers Court
Business Park, Linfield Road
Belfast BT12 5GH

Tel: +44 (0) 844-800-8456
info-uk@proofpoint.com

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