Cyber Trainingsgids

Bescherm uw bedrijf tegen cyberbedreigingen

brother at your side | in[ctrl]

In samenwerking met KnowBe4 Human error. Conquered.

In 2023 waren de wereldwijde gemiddelde kosten van een datalek €4,05 miljoen[1] - een stijging van 15% in 3 jaar.

Is op afstand werken een factor bij het ontstaan van een datalek? Dan zijn de gemiddelde kosten per inbreuk €157.506[2] of hoger.

54% van de bedrijven zegt dat hun IT-afdeling niet geavanceerd genoeg is om intelligente cyberaanvallen af te slaan.[3]

Als hackers nu zouden proberen om uw cyberdefensie te doorbreken, zouden ze dan succesvol zijn? Als u niet op de kracht van de cyberbeveiliging van uw organisatie kunt vertrouwen, heeft u een groot probleem. Maar u bent niet de enige.

Het veilig houden van IT-systemen blijft een van de grootste uitdagingen voor IT Decision Makers (ITDM's). Cyberbedreigingen worden steeds geavanceerder en organisaties zijn meer dan ooit afhankelijk van digitale systemen. Het risico van een succesvolle aanval is nog nooit zo groot geweest.

Uit onderzoek van Brother blijkt helaas dat veel IT-afdelingen onvoorbereid zijn. Gebrek aan budget en de juiste middelen/tools zijn enkele van de meest genoemde redenen waarom veel ITDM's zich zorgen maken over de dreiging van cyberbeveiligingsaanvallen en hun vermogen om zich succesvol te verdedigen.

54% van de ITDM's zegt dat het budget voor beveiliging van IT-systemen stijgt.

Toch vindt 44% nog steeds dat onderhoud en veiligheid van IT-systemen de grootste uitdaging is, wat aangeeft dat budgetten waarschijnlijk niet verstandig worden besteed

We hebben gegevens van Brother gebruikt en zijn een samenwerking aangegaan met KnowBe4 om de risico's binnen bedrijven te belichten. We geven ook aan hoe de implementatie van training en kennis over beveiliging organisaties veilig houden en dat ze daardoor voorbereid zijn op mogelijke bedreigingen.

Mensen zijn de laatste verdedigingslinie als het gaat om de cyberveiligheid van een organisatie. Dat neemt niet weg dat IT-afdelingen uiteindelijk eindverantwoordelijk zijn voor eventuele cyberbeveiligingsproblemen. De realiteit is echter dat ook elke werknemer mee verantwoordelijk is voor het voorkomen van cyberaanvallen. Een integraal onderdeel van de cyberbeveiligingsstrategie van elke organisatie moet er daarom op gericht zijn dat werknemers dit inzien en leren begrijpen. Ze moeten training krijgen om zich bewust te zijn van cyberbeveiligingsbedreigingen en wat ze moeten doen om ze te voorkomen.

Menselijke fouten zijn een belangrijke oorzaak in **95%** van cyberinbreuken.[4]

Basil Fuchs
Chief Information Officer
Brother International Europe

"De risico's voor cyberbeveiliging nemen alsmaar toe. Dat is een direct gevolg van cybercriminelen die steeds geraffineerder worden met social engineering om aanvallen uit te lokken. Mensen krijgen al voorbedachte, valse informatie over scam-e-mails voordat ze in hun inbox terechtkomen, zodat de berichten legitiemer lijken. Cybercriminelen spelen ook in op de behoefte van werknemers om snel te werken en geen tijd te hebben om berichten zorgvuldig te analyseren op signalen van een aanval."

[1]IBM [2]IBM [3]Sophos [4]IIBM Cyber Security Intelligence Index Report

brother at your side | KnowBe4 Human error. Conquered.

De grootste bedreigingen voor bedrijven

Brother deed grondig onderzoek onder IT-managers in Europa en vroeg naar de cyberbeveiligingsrisico's waarmee ze worden geconfronteerd en waarvoor ze zich onvoldoende toegerust voelen. Het zal geen verrassing zijn dat dit allemaal gebieden zijn waar menselijke fouten een rol kunnen spelen.

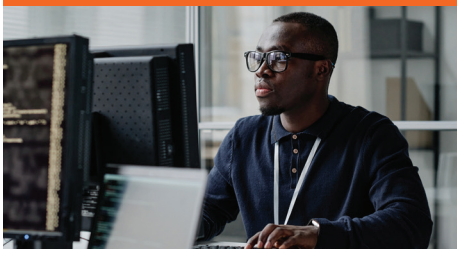
In deze gids kijken we naar de drie meest genoemde cyberdreigingen waartegen ITDM's het minst opgewassen zijn. We laten ook tools en technieken zie die uw organisatie kan gebruiken om de verdediging te versterken en het risico op een beveiligingsaanval te minimaliseren.

Deze bedreigingen zijn:

Phishing-aanvallen

Malware

Netwerkbeveiliging



Omdat veel IT-beslissers niet over de noodzakelijke tijd of het budget beschikken is een van de grootste uitdagingen voor IT-afdelingen om de behoefte aan training over deze onderwerpen aan te bieden. Maar gezien de mens de laatste verdedigingslinie is, moeten alle medewerkers leren hoe ze risico's snel en accuraat kunnen herkennen en hoe ze moeten reageren. Bedrijven zonder veel interne middelen kiezen er vaak voor om partners in de arm te nemen, die de hiaten binnen de cyberbeveiliging kunnen opvullen.

Russell Johnson
Business Partner en Global Cyber Security Lead
Brother International Europe

"Het is gemakkelijk voor bedrijven om te denken dat ze de beveiligingstraining zelf kunnen aanpakken. Een externe partij betrekken bij cyberbeveiliging kan tegen het idee van een effectieve cyberverdediging in lijken te gaan.

Als interne afdeling echter niet op de hoogte zijn van de nieuwste hacktechnieken, kun je werknemers niet succesvol trainen om de cyberverdediging op peil te houden en blijven bedrijfssystemen kwetsbaar voor aanvallen."

Mensen spelen de grootste rol in de beveiliging van een organisatie

We vroegen in ons onderzoek ook naar de meest uitdagende IT-kwesties. 50% van de ITDM's zei dat het onderhouden van veilige IT-systemen steeds moeilijker wordt. Hackers ontwikkelen voortdurend nieuwe tools en technieken om de verdediging van cyberbeveiliging te doorbreken. Voor organisaties is het lastig om de nieuwste benaderingen te herkennen en er effectief bescherming tegen te bieden. Ondertussen zorgt de groei van het Internet of Things (IoT) voor veel nieuwe, potentiële doelen die door hackers kunnen worden aangevallen.

Met zoveel toegangspunten tot een bedrijf en veel werknemers die online werken op meerdere apparaten en locaties, zijn het vaak de mensen binnen een organisatie die de zwakste schakel vormen in de cyberbeveiligingslinie. Gebrek aan training, vergeten of simpelweg niet opvolgen van de beste beveiligingspraktijken, of cybercriminelen die hen in de val lokken, zijn de meest genoemde oorzaken waarom medewerkers het grootste risico vormen van de beveiliging. Maar collega's zijn tegelijktijd ook de grootste troef.

Slechts 29% van de IT-managers zet training met betrekking tot beveiliging bovenaan de prioriteitenlijst.

Slechts 1 op 9 bedrijven in het Verenigd Koninkrijk gaf in 2022 cyberbeveiligingstraining aan het personeel.

Javvad Malik
Lead Security Awareness Advocate
KnowBe4

"Technologie en training zijn nauw verweven in het beveiligingsbewustzijn. Benut digitale hulpmiddelen om mensen uitgebreid op te leiden. Zorg voor interactieve modules, gesimuleerde phishing-oefeningen en toegang tot online informatie, zodat werknemers de principes achter cyberbeveiliging effectief begrijpen. Training kan helpen om kritisch denken en veilige werkmethodes aan te leren, zodat medewerkers bedreigingen herkennen en erop reageren. Al deze zaken samen creëren een dynamische leeromgeving waarin medewerkers niet alleen de risico's van cyberbeveiliging begrijpen, maar ook de vaardigheden ontwikkelen om ze te voorkomen. Regelmatige updates en feedback zorgen voor afstemming op veranderende bedreigingen en bevorderen een cultuur van waakzaamheid en veerkracht binnen de organisatie."

Hackers hebben geen morele bezwaren om organisaties van welke omvang dan ook aan te vallen. Vooral kleine en middelgrote bedrijven die geen grote investeringen doen in defensieve cyberbeveiliging lopen grote risico's. Werken op afstand is de norm geworden en het is voor bedrijven een grote uitdaging om ervoor te zorgen dat medewerkers de beste en veiligste procedures volgen op het gebied van cyberbeveiliging.

Creëer binnen de organisatie een cultuur rondom cybersecurity

Regelmatige cyberbeveiligingstraining zou een integraal onderdeel moeten zijn van de voortdurende professionele ontwikkeling (CPD) van elke werknemer.

Effectieve training op cyberbeveiliging is meer dan werknemers met tussenpozen bewust maken van het probleem. Organisaties die echt voorbereid zijn op aanvallen en de beste verdediging integreren, hebben de beste cyberbeveiligingscultuur en medewerkers die onbewust hun kennis en verdediging voortdurend versterken.

Russell Johnson
Business Partner en Global Cyber Security Lead
Brother International Europe

"Brother zet zich in voor een cyberbeveiligings-cultuur binnen de hele organisatie. We begrijpen dat cyberbeveiliging geen vinkje is. Het is een collectieve en constante verantwoordelijkheid. Onze beveiliging is zo sterk als onze mensen. De beste manier om onze organisatie te beschermen is in werknemers investeren en hen de kennis en vaardigheden te geven om cyberbedreigingen te herkennen en erop te reageren, waar en wanneer ze zich ook voordoen."

60% van de ITDM's binnen het MKB zegt dat de IT-afdeling verantwoordelijk is voor **bedrijfsbrede** training op het gebied van cyberbeveiliging.

Russell Johnson
Business Partner and Global Cyber Security Lead
Brother International Europe

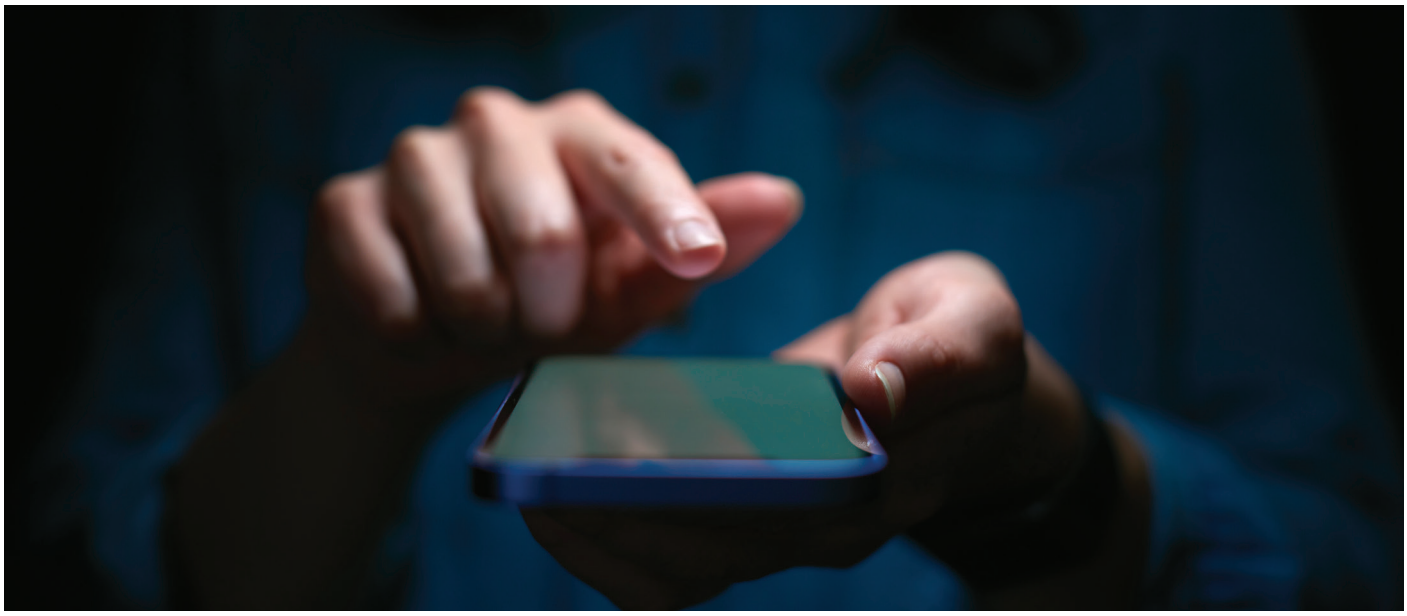
"De afgelopen jaren hebben we ons cyberbeveiligingsbewustzijn binnen Brother drastisch verhoogd met sensibiliseringstests voor beveiligingsvaardigheden en automatische training die zeer doelgericht is en gebaseerd op de geïdentificeerde zwakke punten van gebruikers. We vullen dit aan met tweewekelijkse artikelen op basis van actuele cyberbeveiligingsnieuws en -trends, alsook driemaandelijkse interactieve webinars met gastsprekers om onze afdelingen te betrekken bij de nieuwste ontwikkelingen."

De beste tips om werknemers te betrekken bij cyberbeveiliging

Onderzoek suggereert dat IT-afdelingen verantwoordelijk zijn voor het creëren van een cyberbeveiligingscultuur binnen elke organisatie. Dat kan echter lastig zijn met beperkte kennis en middelen. Elke organisatie moet desondanks stappen ondernemen om zich te beschermen.

Dit betekent:

- Creëer inhoud en trainingsmateriaal die aanslaan bij collega's in het hele bedrijf, op verschillende vaardigheidsniveaus.
- Zorg ervoor dat de inhoud van de training duidelijk en relevant is en gepaard gaat met voorbeelden uit de praktijk.
- Biedt de inhoud aan in een format waar iedereen zich in kan vinden en dat de informatie toegankelijk en eenvoudig maakt.
- Gebruik verschillende technieken om cyberopleiding onderdeel te maken van de bedrijfscultuur, zoals nieuwsbrieven, video's, posters en zelfs evenementen
- Om de grootste impact te realiseren, moeten internationale organisaties er niet alleen voor zorgen dat de inhoud op de juiste manier vertaald is, maar ook regiospecifiek is voor gebruikers.
- Bevorder goede relaties tussen IT en collega's in het hele bedrijf, geef positieve feedback en complimenten aan de werknemers die verdacht gedrag of verdachte e-mails melden, zodat ze zich gewaardeerd voelen voor hun bijdragen.
- Moedig managers aan om hun ervaringen te delen en het goede voorbeeld te geven.



Phishing-aanvallen

Phishing treedt op wanneer een cybercrimineel zich voordoet als een legitieme persoon of bedrijf, vaak via e-mail, sociale media of telefoon, om gevoelige informatie zoals wachtwoorden of creditcardnummers te verkrijgen. Het wordt ook gebruikt om malware te verspreiden. Phishing blijft een van de meest populaire vormen van cyberaanvallen waarbij sociale manipulatie (social-engineering) een rol speelt.

Bij 74% van alle datalekken speelt de menselijke factor een rol.[5]

Aangezien organisaties sterk afhankelijk zijn van digitale communicatiekanalen, bieden deze een ideale kans voor cybercriminelen. Het vermijden van een phishingaanval hangt echter bijna volledig af van het vermogen van werknemers om een phishingaanval te herkennen en te vermijden.

Helaas omvatten phishingzwendel meestal het zich voordoen als bekende merken zoals Microsoft, Amazon, DocuSign en Google om gebruikers te misleiden. In 2022 werden meer dan 30 miljoen berichten met Microsoft-branding of verwijzingen naar Microsoft-producten gebruikt in phishingaanvallen.[6]

28% van de IT-beslissers binnen het MKB geeft aan dat ze zich het minst voorbereid voelen voor phishingaanvallen.

96% van de bedrijven in het Verenigd Koninkrijk vormen het grootste doelwit voor phishingaanvallen in Europa, gevolgd door 94% van de bedrijven in Spanje, 85% in Frankrijk en 79% in Italië.[7]

[5]Verizon's 2023 Data Breach Investigation Report [6]Forbes, 2023 [7]IT Governance

Hoe kunnen bedrijven zichzelf beveiligen tegen phishingaanvallen?

Aangezien phishingaanvallen menselijke zwakheden uitbuiten, is de enige echte manier om uw organisatie ertegen te beveiligen ervoor te zorgen dat alle werknemers goed getraind zijn, zodat ze aanvallen kunnen herkennen en weten wat ze moeten doen als ze er een vermoeden van hebben. En aangezien phishingaanvalmethoden voortdurend veranderen en ontwikkelen, mag training en onderwijs over de nieuwste phishingtechnieken niet worden gezien als een eenmalige gebeurtenis, maar als een regelmatige update die aan alle werknemers wordt gegeven, ongeacht hun rol binnen de organisatie.

Als een extra beschermingslaag kunnen ITDM's ook beschermingssoftwareoplossingen tegen phishing implementeren. Deze werken door verschillende elementen van berichten te analyseren en verdachte inhoud te markeren of te blokkeren, zodat deze uw inbox of webbrowser niet bereikt.

Phishing waarschuwingstekens

Een succesvolle phishingaanval is gebaseerd op de noodzaak om werknemers te misleiden zodat ze klikken op en/of iets delen wat ze niet zouden moeten doen. De enige manier om te voorkomen dat ze dit doen, is door regelmatige training en herhaling van de 'waarschuwingssignalen' die kunnen wijzen op een phishingpoging.

Waarschuwingssignalen waar ze op moeten letten:

- Een bericht dat afkomstig is van een domein dat niet hetzelfde is als het bedrijf waar het zogenaamd van afkomstig is
- Niet-overeenkomende URL's in een webadres
- Spelfouten en grammaticale fouten
- Ongebruikelijke lettertypen, vooral als het lettertype halverwege een woord lijkt te veranderen
- De poging om een gevoel van urgentie te creëren: "deze link verloopt binnen 48 uur" of "haast u om uw identiteit te valideren"
- Ongebruikelijke begroetingen, zoals "Hallo daar".

Hoe goed zijn de medewerkers binnen uw organisatie in het herkennen van een phishing-e-mail of bericht? Vroeger waren phishingberichten redelijk eenvoudig te herkennen dankzij duidelijke spel- en grammaticale fouten. Tegenwoordig maakt generatieve AI het voor scammers echter steeds makkelijker om deze fouten te voorkomen, waardoor het moeilijker wordt om phishingberichten te detecteren. Een manier om erachter te komen hoe goed uw afdelingen zijn voorbereid, is door het Phish-prone™ percentage binnen de organisatie vast te stellen.

Regelmatige phishingtests zouden daarom een integraal onderdeel moeten vormen van het cyberbeveiligingsplan van elke organisatie.

Russell Johnson
Business Partner en Global
Cyber Security Lead
Brother International Europe

We hebben verschillende zaken geïmplementeerd om het risico op een phishingaanval te minimaliseren. Enkele van de phishing-simulaties die we als onderdeel van onze cyberstrategie hebben ingezet zijn:

- E-mails die afkomstig lijken te zijn van HR, met onderwerpen zoals ziekte, jaarlijks verlof en het ondertekenen van nieuwe beleidsregels.
- E-mails die afkomstig lijken te zijn van managers, zoals het vragen aan medewerkers om snel documenten te openen, te lezen of te ondertekenen.
- E-mails die afkomstig lijken te zijn vanuit het systeem, zoals links om een Google doc te ondertekenen of toegang tot een SharePoint.

Phish-prone™ percentage: Wat is het en waarom is het belangrijk?

Het Phish-prone percentage verwijst naar het percentage werknemers dat geneigd is om op een phishinglink te klikken of op een onveilige manier te reageren op een phishingbericht. Dit kan zijn door gegevens in te voeren op een nep-landingspagina, een bijlage te openen of op het bericht te reageren.

Het Phish-prone™ percentage wordt berekend door het aantal werknemers dat in een phishingtest is getrapt te delen door het totale aantal geteste werknemers. Het resultaat wordt vervolgens vermenigvuldigd met 100 om het percentage te verkrijgen. Bijvoorbeeld, als een organisatie 100 werknemers heeft en 20 van hen klikten op een phishing-e-mail tijdens een test, zou het phish-prone percentage 20% zijn.

"Raak niet in paniek als uw Phish-prone score hoger is dan u verwacht - het is vrij gebruikelijk als u nog niet eerder phish-tests heeft gedaan. Bij Brother hebben we onze score aanzienlijk kunnen verlagen in een relatief korte tijd met behulp van een reeks trainingstools en gesimuleerde phishingtests. In feite behalen we nu onze branchebenchmark van 6%, wat het effect aantoont dat constante tests en regelmatige training kunnen hebben."

Phishingtests en -training in de praktijk

Phishingtests zijn een van de meest effectieve manieren om te ontdekken hoe goed afdelingen binnen uw bedrijf zijn voorbereid op een phishingaanval en zorgen ervoor dat de Phish-prone score van uw organisatie verlaagd wordt. Het principe is eenvoudig. Bedrijven die personeel willen testen, maken en versturen gesimuleerde phishingtests. Dit kan zowel intern als via een gespecialiseerd bedrijf. Deze tests proberen medewerkers te misleiden om gevoelige informatie te geven, maar zonder enig echt risico. Er zijn meerdere manieren waarop ze proberen deze informatie te verkrijgen, en aan het einde van de tests wordt de Phish-prone percentage berekend en vergeleken met andere bedrijven binnen uw branche (een benchmarkcijfer).

Javvad Malik
Lead Security Awareness Advocate
KnowBe4

"Uit het Phishing by Industry Benchmarking Report 2023 van KnowBe4 blijkt dat 33,2% van de ongetrainde gebruikers niet zal slagen voor een phishing-test. Door beveiligingstrainingen te implementeren en zich in te zetten voor de ontwikkeling van een cultuur van cyberbeveiliging hebben bedrijven echter aangetoond dat het mogelijk is dit terug te brengen tot onder de branchenorm van 5,9%."

Russell Johnson
Business Partner and Global Cyber Security Lead
Brother International Europe

"Bij Brother hebben we ons percentage dat vatbaar is voor phishing de afgelopen jaren consequent verlaagd. Hoe? We zijn in maart 2022 begonnen met een baseline phishing-test, waaruit bleek dat ons Phish-prone Percentage (PPP) 11,5% bedroeg. Hierna hebben we robuuste training en veiligheidsbewustzijnstests geïmplementeerd om de belangrijkste zwakke punten te identificeren. Op basis hiervan konden we passende trainingen geven om eventuele hiaten op te vullen. We hebben meer dan 30.000 phishing-e-mails verstuurd, waarvan 17.000 in de afgelopen twaalf maanden. Op dit moment bedraagt onze PPP slechts 5,2%, met een doelstelling van <2%."

De branchebenchmark voor phishing is opgebouwd in drie fasen:

Fase één: Een gesimuleerde phishing-e-mail wordt naar alle gebruikers gestuurd die geen eerdere training hebben gehad. Het percentage werknemers dat in de phishing-e-mail trapt, is het basispercentage. Gemiddeld zal wereldwijd 33,2% van deze groep slachtoffer worden van deze phishing-e-mail.

Fase twee: 90 dagen na fase één, hebben gebruikers training gevolgd en phishingtests ontvangen.

Fase drie: De test wordt na 12 maanden herhaald.

Wat de gegevens laten zien, gebaseerd op 32,1 miljoen phishing-e-mails naar 12,5 miljoen gebruikers, is dat de resultaten van phishing-beveiligingstests na 90 dagen training wereldwijd dalen van 33,2% naar 18,5%. Dit daalt verder tot 5,4% na 12 maanden.

Deze percentages variëren afhankelijk van de branche, locatie en omvang van de organisatie.

91% van de geslaagde datadiefstallen begint met een spearphishing-aanval.[9]

Wat is spearphishing?

Spearphishing is een soort phishing-aanval die zich richt op specifieke individuen of organisaties, meestal via kwaadaardige e-mails. Het doel van spearphishing is het stelen van gevoelige informatie, zoals inloggegevens, of het infecteren van het apparaat van het doelwit met malware.

[8]KnowBe4 [9]KnowBe4

Malware

Een van de grootste uitdagingen waarmee ITDM's te maken krijgen, is de dreiging van een zeer specifiek type software, genaamd malware, dat hun IT-infrastructuur binnendringt.

34% van de IT-verantwoordelijken in het MKB zegt dat malware/ransomware de beveiligingsdreiging is waarvoor ze zich het minst voorbereid voelen.[10]

Wat is Malware?

Malware is software die specifiek is ontworpen met als doel het verstoren, beschadigen of ongeautoriseerde toegang verkrijgen tot een computersysteem. Zoals we weten, worden phishing-aanvallen vaak gebruikt om malware op uw systemen te krijgen – dit gebeurt meestal door op een link in een phishing-bericht te klikken of bijlagen te downloaden waarvan u niet weet dat ze schadelijk zijn.

Andere manieren waarop malware toegang kan krijgen tot uw apparaat:

- Automatische downloads vanaf schadelijke websites
- Geïnfecteerde software die op uw apparaat wordt geïnstalleerd
- Verwisselbare media: USB-drives en externe harde schijven
- Verouderde software met beveiligingsproblemen

December 2023 werden in Europa meer dan **100,884,532** gegevens gestolen.[11]

[10]2023 Brother X Savanta ITDM-prioriteitonderzoek [11]IT-beheer

De gevaarlijkste soorten malware: een overzicht

Trojaanse paarden

Een Trojaans paard is een virus dat uw bestanden kan beschadigen, gegevens kan wijzigen, activiteiten kan controleren, gevoelige bestanden en informatie van uw apparaat kan stelen, internetverkeer kan omleiden of zelfs een achterdeur van uw systemen kunt openzetten – allemaal zonder uw medeweten.

Ransomware

Ransomware is schadelijke software die is ontworpen om de toegang tot uw apparaat en de daarop opgeslagen gegevens te blokkeren totdat u losgeld aan de aanvaller betaalt. Meestal doen ze dit door uw bestanden te versleutelen, zodat u ze niet langer kunt zien of gebruiken.

Wormen

Wormen zijn een soort Trojaans virus, maar hun voornaamste functie is het zichzelf vermenigvuldigen en andere apparaten te infecteren, terwijl ze ook actief blijven op systemen die ze eerder hebben geïnfecteerd.

Hoe kunnen ITDM's zichzelf beschermen tegen ransomware-aanvallen?

In januari 2023 werd Royal Mail aangevallen door een van de gevaarlijkste ransomwares ter wereld – LockBit – waarvoor een losgeld van 80 miljoen dollar werd geëist.[12]

Zoals we weten, worden veel ransomware-aanvallen uitgevoerd via succesvolle phishing-aanvallen, waarbij gebruikers op onwettige links klikken die onveilige software op hun apparaat downloaden. Dit betekent dat een van de meest effectieve manieren om uw organisatie tegen dit soort bedreigingen te beveiligen, is ervoor te zorgen dat uw medewerkers weten hoe ze phishing-aanvallen kunnen herkennen en vermijden. Daarnaast kunt u samenwerken met een vertrouwde partner die u precies kan vertellen hoe effectief uw afdelingen zijn in het identificeren ervan.

Andere stappen die u kunt nemen om ransomware-aanvallen te voorkomen, zijn:

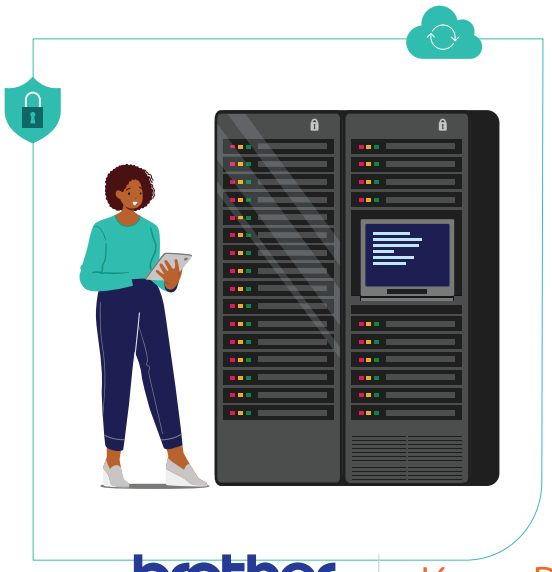
- Software up-to-date houden
- Implementatie van tweefactorauthenticatie, vooral voor externe medewerkers
- Vraag gebruikers om hun wachtwoorden regelmatig te wijzigen
- Gebruik beveiligingshardware en -software, waaronder firewalls, toepassingen voor het scannen van e-mail en antivirussoftware
- Voer regelmatig back-ups uit en bewaar alles in een aparte netwerkomgeving.

Een andere optie is het gebruiken van SOAR - Security Orchestration Automation and Response. SOAR, dat speciaal gemaakt is voor het reageren op en beheren van phishing-bedreigingen, kan de tijd die u nodig heeft om te reageren verkorten (Mean Time To Respond - MTTR). Daarnaast kan het phishing-bedreigingen aanpakken voordat ze de e-mailboxen van uw team bereiken.13 Deze proactieve houding ten opzichte van phishing wordt verder ondersteund door mogelijkheden zoals:

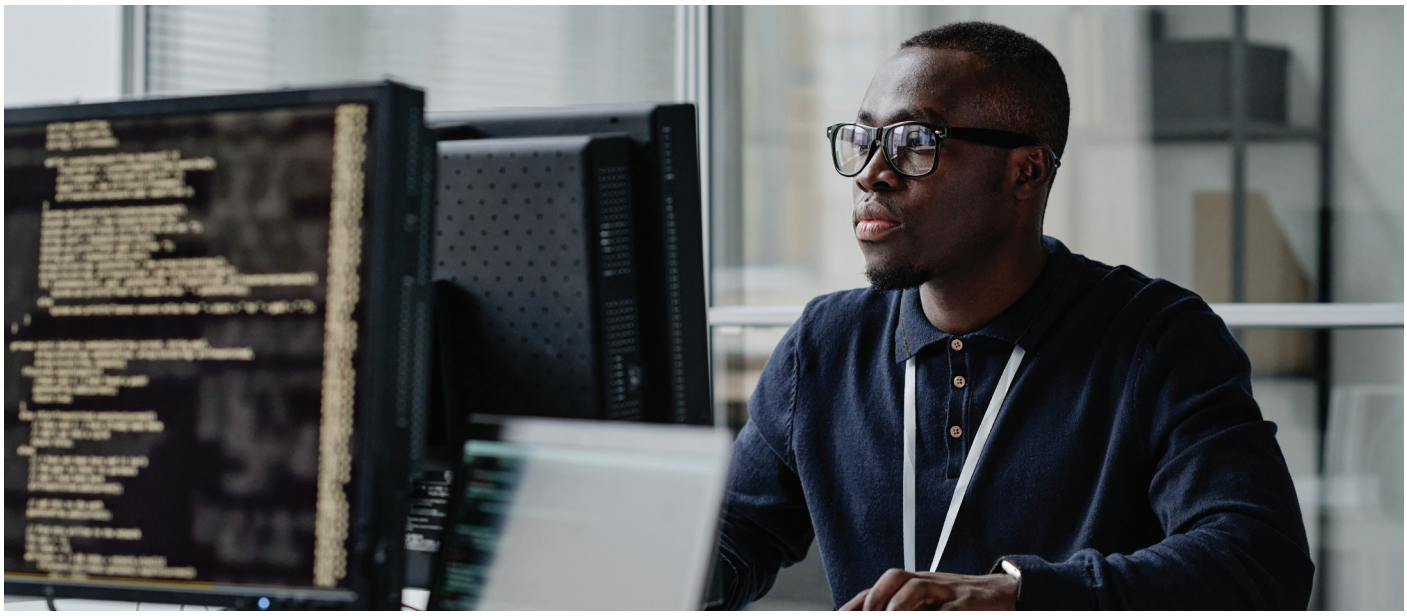
- Geautomatiseerde e-mail-alarmberichten waarmee IT-afdelingen de andere teams snel op de hoogte kunnen brengen van eventuele gevaren
- Patroonidentificatie waarmee het incidentresponsteam wijdverspreide aanvallen snel kan opsporen
- Aanvallen uit de echte wereld omzetten in simulaties van trainingsmodellen om zo de vaardigheden en ervaring van werknemers te verbeteren.

Javvad Malik
Lead Security Awareness Advocate
KnowBe4

"Om ransomware te verslaan, kunnen organisaties tools als RanSim gebruiken om een 360° beeld te krijgen in welke mate zij voorbereid zijn op een aanval. RanSim simuleert 24 verschillende ransomware-infectiescenario's en één cryptomining-infectiescenario om te bepalen of een werkstation kwetsbaar is."



[12]bbc.co.uk [13]KnowBe4



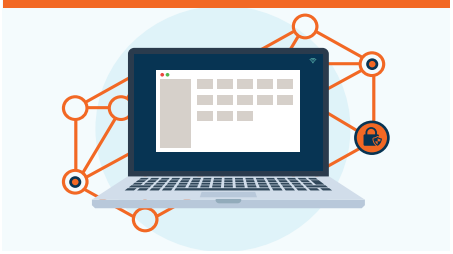
Netwerkbeveiliging

Iets dat vaak over het hoofd wordt gezien door bedrijven, is netwerkbeveiliging. We weten dat dit een zaak is die grote gevolgen kan hebben. Uit ons onderzoek blijkt duidelijk dat dit vaak een blinde vlek op de prioriteitenlijst is. Netwerkbeveiliging heeft betrekking op de processen en software die u gebruikt om uw computers, printers, netwerk en gegevens te beschermen. Het wordt over het algemeen onderverdeeld in drie gebieden:

Fysiek

Beveiligingscontroles worden gebruikt om ongeautoriseerde toegang tot fysieke systemen zoals printers, routers en harde schijven (endpoints) tegen te houden.

Technisch



Beveiliging die gegevens beschermt die binnenkomen, uitgaan en op het netwerk worden opgeslagen.

Administratief

Beveiligingscontroles voor gebruikersgedrag, zoals wie toegang heeft en welke authenticatiestappen worden gebruikt.

Het minst veilige deel van elk netwerk is het eindpunt. Nogmaals, dit is waar gebruikers in het spel komen. Hybride werken heeft nieuwe uitdagingen gecreëerd voor de netwerkbeveiliging van organisaties. Externe werknemers hebben waarschijnlijk toegang tot bedrijfsservers via openbare netwerken, wat veel minder bescherming biedt. Er is een groter aanvalsoppervlak met meer toegangspunten voor cybercriminelen. Het is ook moeilijker voor IT-afdelingen om aanvallen te identificeren en erop te reageren.

Basil Fuchs
Chief Information Officer
Brother International Europe

"In de digitale en flexibele werkomgeving van vandaag is het belangrijk om netwerken te beveiligen om gevoelige gegevens te beschermen. Het Zero-Trust-model vertrouwt niemand automatisch en controleert alle gebruikers en apparaten voordat ze toegang krijgen. Door toegang te beperken tot alleen wat nodig is, verkleint deze aanpak het risico op ongeautoriseerde toegang binnen het netwerk."

Zero-trust-netwerktoegang is een zeer effectief beveiligingsmodel dat ervoor zorgt dat gebruikers alleen de toegang en machtigingen hebben die nodig zijn om hun werk uit te voeren. Het is een heel andere benadering dan standaard VPN's die alle gebruikers toegang geven tot het volledige netwerk. Het voordeel van een zero trust-benadering is dat als een gebruiker wordt gehackt, kwaadwillenden alleen toegang hebben tot de gegevens die zij kunnen bereiken, en niet tot het gehele netwerk.

We hebben enkele quick-wins samengesteld over manieren om uw netwerkbeveiliging te verbeteren:

1. Gebruik SSL-certificaten
2. Vraag externe medewerkers om hun draadloze thuisnetwerk te coderen met WPA2-versleuteling
3. Wijzig de naam en het wachtwoord van uw router om uw identiteit te maskeren
4. Schakel WPS op routers uit
5. Stuur herinneringen naar alle gebruikers om regelmatig een back-up te maken van hun apparaten, inclusief printers, scanners, enz., en om updates te installeren zodra deze beschikbaar zijn.

Hoe kunt u de netwerkbeveiliging verbeteren?

Netwerkbeveiliging omvat veel verschillende elementen, die allemaal even cruciaal zijn. Dit geldt met name in het tijdperk van hybride werken en werken op afstand, waar het voor ITDM's simpelweg niet mogelijk is om thuiskantoren te bezoeken en te controleren, of collega's binnen de organisatie met enige regelmaat persoonlijk te zien. Met dit in gedachten volgen hier onze beste tips om ervoor te zorgen dat u aan alle eisen voldoet.

Gebruik SSL-certificaten

Een SSL-certificaat (Secure Sockets Layer) en het gebruik van HTTP als u via uw netwerk producten verkoopt, zijn essentieel. Een SSL-certificaat zorgt ervoor dat gegevens die worden gedeeld tussen uw servers en clients niet kunnen worden gestolen door een derde partij. Het certificaat bevestigt de identiteit van de server en zet een gecodeerd communicatiekanaal op om online aankopen mogelijk te maken.

Houd uw routerfirmware up-to-date

Dit is vooral belangrijk voor externe medewerkers, omdat routerfirmware vooraf op hun apparaten is geïnstalleerd. Routerfirmware moet minstens één keer per jaar worden bijgewerkt om de beste verdediging tegen cyberdreigingen te bieden.

Gebruik WPA2

Wi-Fi Protected Access2, of WPA2, is een van de sterkste en meest complexe beveiliging algoritmen om uw Wi-Fi-netwerk te beveiligen.

Implementeer een VPN

Virtual Private Networks, of VPN's, zijn essentieel voor externe medewerkers, omdat ze het risico verkleinen dat informatie wordt onderschept terwijl deze tussen netwerken wordt uitgewisseld. VPN's beschermen thuiswerkers tegen onbedoeld gebruik van kwetsbare openbare netwerken.

Breng firewalls in de lucht

Het lijkt misschien voor de hand liggend, maar sterke firewalls zijn nog steeds een van de meest effectieve cyberbeveiligingswapens in uw arsenaal. Zorg ervoor dat u zowel een interne als een externe firewall heeft en kijk naar de gelaagdheid van hardware- en softwaregebaseerde firewalls en zorg ervoor dat deze regelmatig worden bijgewerkt voor de beste bescherming.

Schakel het delen van bestanden uit

Hoewel samenwerking van fundamenteel belang is voor externe medewerkers, biedt het delen van bestanden een reële kans voor hackers om toegang te krijgen tot gevoelige informatie of om schade aan uw systemen te veroorzaken. Het implementeren van cloudgebaseerde of met een wachtwoord beveiligde systemen maakt samenwerking mogelijk zonder uw netwerk kwetsbaar te maken.

Beveilig endpoints

Printers en andere plug-in apparatuur zoals scanners en draagbare harde schijven worden vaak over het hoofd gezien als het gaat om netwerkbeveiliging. Zorg ervoor dat de software up-to-date is en overweeg voor printer een Secure Print oplossing – een functie waarmee gebruikers het daadwerkelijke afdrukken kunnen uitstellen totdat ze fysiek voor de printer staan.

Printerbeveiliging

Een onderdeel van het eindpuntbeveiliging dat vaak over het hoofd wordt gezien, is printerbeveiliging. Printers lijken vaak redelijk veilige apparaten, maar kunnen door hackers worden gebruikt als achterdeur naar uw netwerk. En dit gebeurt vaker dan u zou verwachten.

Bij ruim één op de tien beveiligingsincidenten die bedrijven treffen, is een printer betrokken.[14]

Dat komt omdat de meeste moderne printers met internet zijn verbonden en deze netwerkverbinding in twee richtingen werkt: van uw apparaat naar uw printer, maar ook van uw printer terug naar uw apparaat. En hoewel gebruikers niet lang hoeven na te denken over het afdrukken van gevoelige informatie, kan deze tweerichtingsverbinding door slimme hackers worden misbruikt als uw printer niet over hetzelfde niveau van beveiliging beschikt als uw computer.

Volgens onderzoek van Brother maakt 95% van alle organisaties zich zorgen over de netwerk beveiliging voor hun hybride werknemers.

Security by Brother is onze op oplossingsgerichte benadering van endpointbeveiliging die zakelijk printen veilig maakt. We bieden beveiliging op drie levels: netwerk-, apparaat- en documentniveau. Zo kunnen wij ervoor zorgen dat uw informatie alleen wordt gezien door degenen waarvoor deze bedoeld is.

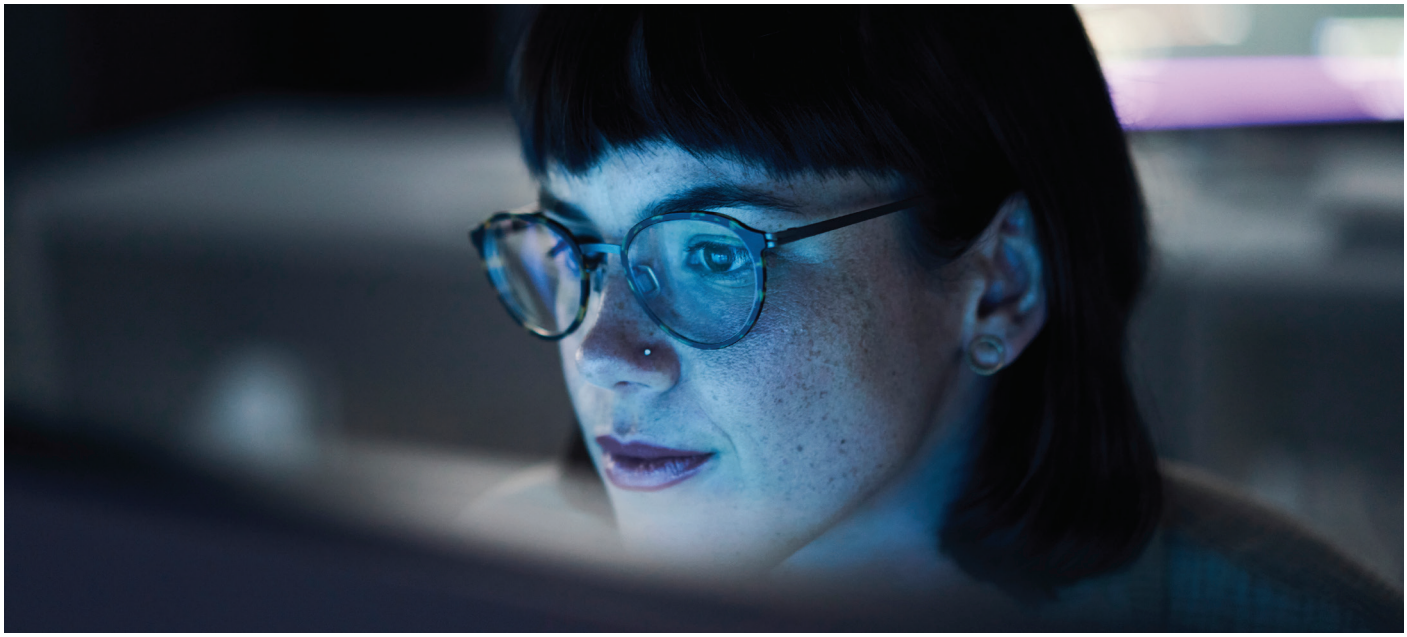
[14]Quocirca.

En tot slot...

We hebben gezien dat een ‘must have’ en ‘nice to have’ benadering van risicoreductie de beste methode is om ervoor te zorgen dat het IT-budget effectief wordt besteed. We kunnen deze opsplitsen in:

Noodzakelijke voorwaarden: elementen die essentieel zijn voor succes, zoals een geconfigureerde firewall, antivirussoftware, VPN’s, basistraining cybersecurity en wachtwoordmanagers.

Toegevoegde waarde: eelementen die nuttig zouden zijn, maar niet essentieel zijn om een basisniveau van cyberbeveiliging te bieden, zoals multi-factor authenticatie en regelmatige trainingssessies.



Nadat u de grootste risico’s van uw organisatie in kaart heeft gebracht, kunt u met deze methode bepalen welke beveiligingsmaatregelen cruciaal en noodzakelijk zijn om uw organisatie veilig te houden, en welke als toegevoegde waarden zeer voordelig kunnen zijn als er hiervoor ruimte binnen het budget is. Deze methode is voor IT-managers ook een goede manier om te onderbouwen waarom er een budget of extra budget nodig is voor de beveiliging en verdediging van de organisatie.

Uiteindelijk is cyberbeveiliging niet zomaar een lijst met routinematige trainingen voor de mensen binnen uw organisatie. Om uw systemen en gegevens veilig te houden, moet cyberbeveiliging een manier van leven worden voor uw medewerkers – waarbij het opmerken van cyberrisico’s net zo natuurlijk wordt als het opmerken van verkeersrisico’s tijdens het rijden.

Wees bewust van cyberdreiging

Bent u geïnteresseerd in beveiligd printen, neem dan contact op met onze specialisten.

brother at your side | in[ctrl]

In samenwerking met KnowBe4 Human error. Conquered.