MX-Relay

Protecting E-mail

Snel • Eenvoudig • Betrouwbaar

13 soorten e-mailbedreigingen die u nu moet kennen

Hoe Inbox Defense beschermt tegen steeds geavanceerdere aanvallen

MX-Relay • Taag 77, 2491 CS Den Haag • +31 (0)70 320 67 94 • sales@mx-relay.com

MX-Relay

Inhoudsopgave

MX-Relay

Inleiding: Verminder de gevoeligheid voor gerichte e-mailaanvallen radicaal

Een cyberaanval kan uw bedrijf op vele manieren beïnvloeden, afhankelijk van de aard, omvang en ernst ervan.

Volgens het FBI's internet Crime Complaint Center (iC3) kostte cybercriminaliteit alleen al in 2019 $3,5 miljard aan verliezen, waarbij zakelijke e-mail overname (beC) de meeste schade veroorzaakte. Dit aantal is exclusief niet-gemelde verliezen, die aanzienlijk zijn. IC3 ontving vorig jaar 467.361 klachten - meer dan 1.300 per dag - waarbij Phishing verantwoordelijk was voor 93 procent van de e-mailinbreuken. Bij een cyber aanval worden ook indirecte en immateriële kosten gemaakt, zoals juridische kosten, boetes voor regelgeving, operationele verstoringen, een beschadigde merkreputatie en andere ernstige gevolgen.

In de snel evoluerende omgeving van vandaag volstaan traditionele e-mailbeveiligingsoplossingen niet meer om bedrijven te beschermen. U moet zich ook effectief verdedigen tegen geavanceerde e-mailbedreigingen die de beveiliging vaak kunnen omzeilen door achterdeurtechnieken, waaronder spoofing, social engineering en fraude, welke worden gebruikt om netwerken binnen te dringen en schade aan te richten.

Terwijl uitgebreide e-mailgateway defenses een solide basis bieden, vermindert het gebruik van een meerlaagse beschermingsstrategie de gevoeligheid voor e-mailaanvallen radicaal en helpt het uw bedrijf, gegevens en mensen beter te beschermen.

Deze whitepaper gaat dieper in op de belangrijkste typen e-mailbedreigingen, inclusief hun risico's en impact op bedrijven, en hoe AI en API-gebaseerde inbox defense de hiaten in de e-mailgateway kunnen aanpakken en kunnen helpen bij het bieden van totale e-mailbescherming tegen aanvallen.

"Tot 2023 zullen de BEC-aanvallen elk jaar blijven verdubbelen tot meer dan $ 5 miljard en leiden tot grote financiële verliezen voor ondernemingen."

MX-Relay

Steeds complexere e-mailaanvallen bestrijden

De e-mail- en phishing-bedreigingen waarmee organisaties tegenwoordig worden geconfronteerd, variëren sterk in complexiteit, volume en de impact die ze hebben op bedrijven en hun werknemers. Er zijn een aantal verschillende categorieën van e-mailbedreigingen;

Spam
Ongevraagde berichten met een hoog volume, doorgaans van commerciële aard, die worden verzonden zonder rekening te houden met de identiteit van de ontvanger.

Malware
Software die speciaal is ontworpen om schade aan technische activa te veroorzaken, activiteiten te verstoren, gegevens te exfiltreren of anderszins toegang te krijgen tot een systeem op afstand. Malware wordt meestal verspreid via e-mailbijlagen of URL's die tot schadelijke inhoud leiden.

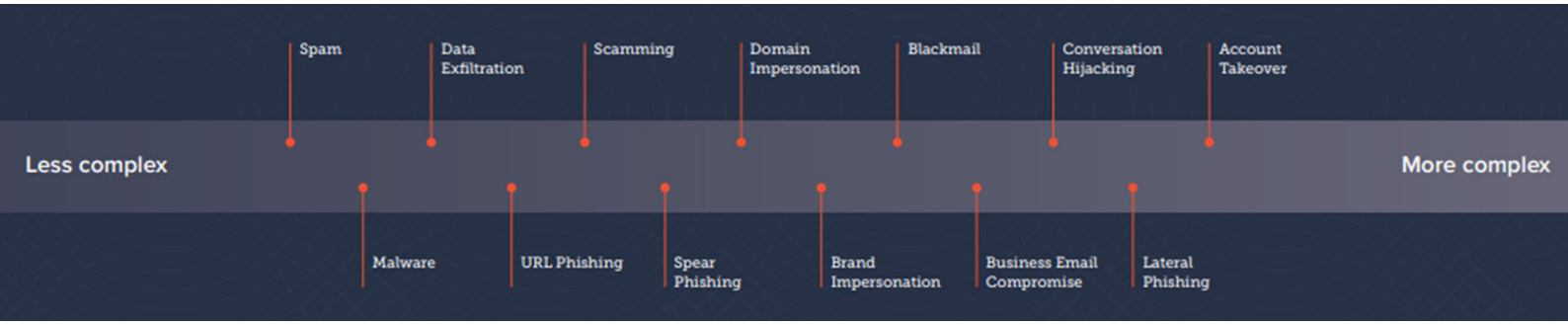
Data exfiltratie
Dit soort aanvallen vinden plaats wanneer gegevens zonder toestemming van de eigenaar worden gekopieerd of opgehaald van een extern systeem. Het kan kwaadwillig of per ongeluk gebeuren.

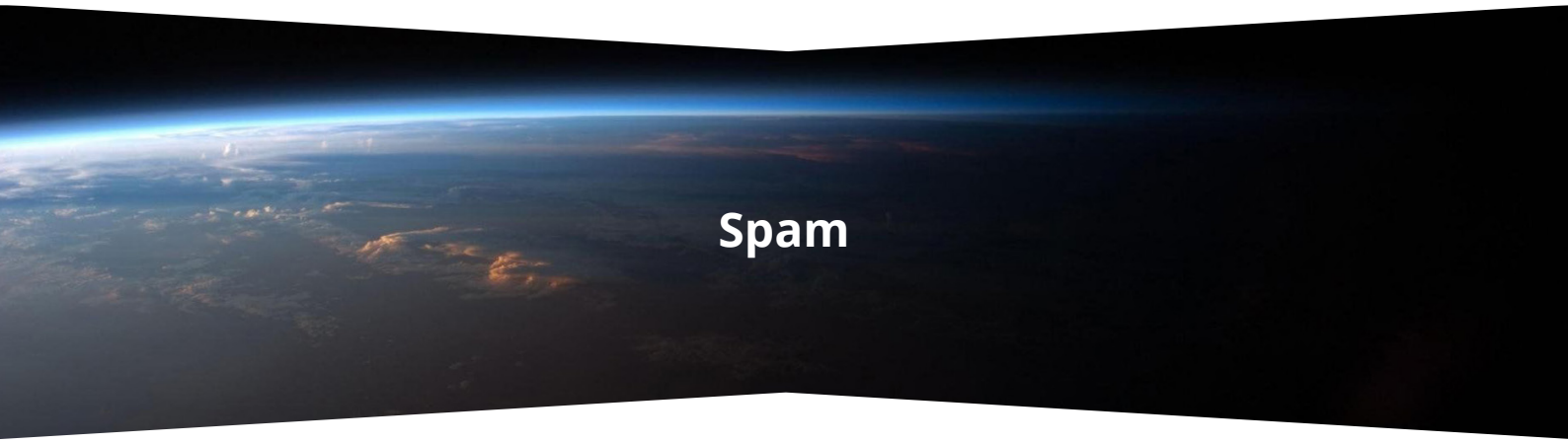
Phishing
Deze e-mails proberen een eindgebruiker te laten geloven dat het bericht afkomstig is van een vertrouwd persoon of organisatie. Met als doel diegene actie te laten ondernemen, zoals het bekendmaken van inloggegevens, het overmaken van geld of het inloggen op een legitiem account namens een aanvaller.

Nabootsing van identiteit
Deze categorie omvat elke aanval waarbij de kwaadwillende zich voordoet als een persoon, organisatie of dienst. Het is een breed scala aan aanvallen die meestal samen gaan met phishing.

In totaal vallen er 13 typen e-mailbedreigingen in deze categorieën. Sommige van deze aanvallen worden in combinatie met andere gebruikt; hackers combineren vaak verschillende technieken. Veel spamberichten bevatten bijvoorbeeld phishing-URL's. Het is niet ongebruikelijk dat een gecompromitteerd account wordt gebruikt bij interne of laterale fraude.

Hier volgt een overzicht van de top 13 typen e-mailbedreigingen en hoe u uw e-mailbeveiliging tegen hen kunt versterken. Naarmate e-mailaanvallen complexer worden, worden ze moeilijker te verdedigen.



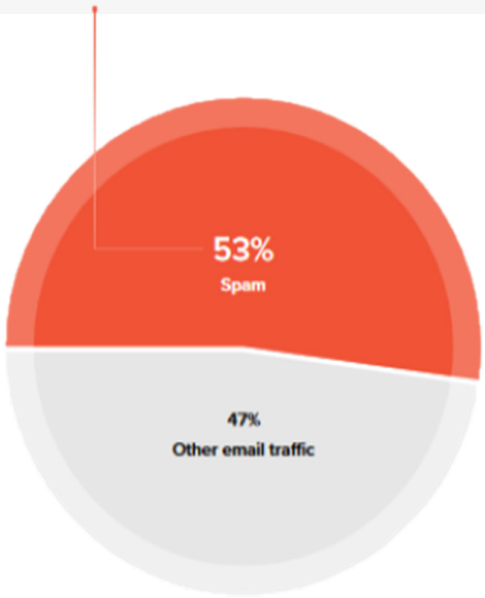


Spam

Spam zijn ongevraagde e-mailberichten, ook wel ongewenste e-mail genoemd. Spammers sturen doorgaans een e-mail naar miljoenen adressen, in de verwachting dat slechts een klein aantal op het bericht zal reageren. Spammers verzamelen e-mailadressen uit verschillende bronnen. De verzamelde e-mailadressen worden vaak verkocht aan andere spammers.

Spam komt in verschillende vormen voor. Spam e-mails pushen oplichting of worden gebruikt om e-mailfraude te plegen. Spam komt ook voor in de vorm van phishing-e-mails die gebruik maken van merk imitatie om gebruikers ertoe te verleiden persoonlijke informatie, zoals inloggegevens en creditcardgegevens, te onthullen.

De impact van spam kost bedrijven ongeveer 20 miljard dollar per jaar aan verliezen.



Doordat de inboxen overspoeld worden met junkmail heeft het ook effect op de productiviteit. Het serververkeer verwerkt op deze manier namelijk berichten minder snel. Spam kan worden gebruikt om malware te verspreiden en bij grootschalige phishing-aanvallen.

Versterking van e-mailbescherming tegen spam
Moderne gateways zijn zeer effectief in het blokkeren van spam; Inline implementatie van spamfilters helpt spam te stoppen voordat het de inbox bereikt. Op API gebaseerde inbox defense is niet zo effectief tegen deze grootschalige aanvallen. Volumineuze aanvallen, zoals spam, kunnen e-mailservers overweldigen en de prestaties van de inbox nadelig beïnvloeden, waardoor een grote inbox-belasting wordt gecreëerd voordat ze worden teruggevorderd door API's.

"Spam is verantwoordelijk voor 53% van het wereldwijde e-mailverkeer en voor ongeveer $ 20 miljard aan verliezen per jaar."

MX-Relay

Malware

Cybercriminelen gebruiken e-mail om documenten te bezorgen die schadelijke software bevatten, ook wel Malware genoemd. Meestal is de Malware rechtstreeks in het document zelf verborgen of downloadt een ingesloten script deze van een externe website. Veel voorkomende soorten Malware zijn virussen, Trojan horse, spyware, worms en ransomware.

Veelvoorkomende soorten Malwareaanvallen

Volumetrische malware

Dit type Malware is ontworpen om massaal te worden verspreid en om te profiteren van oudere systemen met veelvoorkomende kwetsbaarheden. Het maakt gebruik van bekende kwetsbaarheden en kan over het algemeen worden onderschept door middel van handtekeningen welke onjuist blijken te zijn. Volumetrische malware staat ook bekend als: commodity-Malware en virussen.

Zero-day Malware

Geavanceerde Malwareaanvallen maken gebruik van zero-day-bedreigingen. Dit zijn nog eerder geziene bedreigingen. Deze komen niet overeen met bekende Malware. Ze kunnen misbruik maken van een voorheen onbekende kwetsbaarheid in software of maken gebruik van een nieuwe Malwarevariant die met standaardmiddelen wordt geleverd. Deze zero-day-aanvallen zijn onmogelijk te detecteren met traditionele, op handtekeningen gebaseerde oplossingen. Zero-day-Malware staat ook bekend als: 0Day.

URL-aanvallen

URL's die verwijzen naar kwaadaardige websites of payloads zijn over het algemeen bedoeld om gebruikers te misleiden om te klikken om malware te downloaden. Met payload wordt de informatie bedoeld die over een computernetwerk getransporteerd dient te worden en het doel van het transport vormt.

Impact van Malware

Bijna 94 procent van de Malware wordt geleverd via e-mail. Door middel van ransomware, één van de meest populaire vormen van malware, infecteren cybercriminelen het netwerk en vergrendelen ze e-mail gegevens en andere kritieke bestanden totdat er losgeld wordt betaald. Deze evoluerende en geavanceerde aanvallen zijn schadelijk en kostbaar. Ze kunnen de dagelijkse operaties verlammen, chaos veroorzaken en leiden tot financiële verliezen zoals downtime, losgeld, herstelkosten en andere gebudgetteerde en onverwachte uitgaven.

In 2019 zouden de kosten van ransomware mogelijk 170 miljard dollar bedragen. Dit aantal omvat niet alleen het uitgekeerde losgeld, maar ook het verlies aan productiviteit, gegevens en andere schade die de aanval heeft veroorzaakt. De gemiddelde hoeveelheid losgeld is meer dan verdubbeld van $41.198 in het derde kwartaal van 2019 tot $84.000 in het vierde kwartaal van 2019. Er waren in 2019 veel ransomware-aanvallen op bedrijven en overheidsorganisaties. Bij aanvallen van ransomware door de overheid waren lokale, provinciale en deelstaatregeringen allemaal doelwitten, waaronder scholen, gezondheidszorg, bibliotheken, rechtbanken en andere entiteiten.

E-mailbeveiliging tegen Malware

Malwarebescherming kan het beste worden gedaan op gateway-niveau, voordat e-mails de inbox bereiken. Het matchen van handtekeningen blijft een belangrijk hulpmiddel om de meeste Malwarevarianten te detecteren en te blokkeren. Er zijn echter meer geavanceerde technieken beschikbaar om zero-day-bedreigingen te detecteren. Sandboxing is zo'n tool: verdachte bestanden en links worden geanalyseerd in een geïsoleerde testomgeving om er zeker van te zijn dat ze veilig zijn voordat ze in de inbox van gebruikers worden afgeleverd. Nieuwe Malware-handtekeningen kunnen worden gemaakt op basis van sandbox-analyse om toekomstige aanvallen te helpen voorkomen.

Data exfiltration

Data-exfiltratie is de ongeoorloofde overdracht van gegevens van een computer of ander apparaat. Dit kan handmatig worden uitgevoerd via fysieke toegang tot een computer of als een geautomatiseerd proces met behulp van kwaadaardige programmering op he internet of een netwerk. Aanvallen zijn meestal gericht, met als doel toegang te krijgen tot een netwerk of machine om specifieke gegevens te lokaliseren en te kopiëren. Naast kwaadaardige aanvallen gaan gegevens vaak per ongeluk verloren als gevolg van menselijke fouten. Data-exfiltratie staat ook bekend als: data-extrusie, data-export, data-lekken, data-lekkage, data-verlies en data-diefstal.

Impact van data-exfiltratie
Volgens een jaarlijkse IBM rapport zijn de gemiddelde totale kosten van een datalek in 2019 $3,92 miljoen. Voor sommige sectoren, zoals de gezondheidszorg, kan dit aantal bijna verdubbelen. Datalekken in de Verenigde Staten waren het duurst, met een gemiddelde kostprijs van 8,19 miljoen dollar. De gemiddelde omvang van een datalek was 25.575 records. Dataverlies kan leiden tot financiële verliezen en een langdurige impact hebben op de reputatie van een organisatie.

E-mailbeveiliging tegen data-exfiltratie
Veilige e-mailgateways worden in lijn met de e-mailstroom ingezet; ze filteren zowel inkomende als uitgaande berichten. Preventie van gegevensverlies (data loss provention) is een reeks technologieën in combinatie met het bedrijfsbeleid, om ervoor te zorgen dat eindgebruikers geen gevoelige of vertrouwelijke gegevens naar buiten sturen. Een dlp-systeem scant alle uitgaande e-mail op vooraf bepaalde patronen die kunnen wijzen op gevoelige gegevens, waaronder creditcardnummers, Burgerservicenummers en medische termen van HIPAA. Berichten die dit soort gevoelige gegevens bevatten, worden automatisch versleuteld.

URL phishing

Bij phishing-aanvallen proberen cybercriminelen gevoelige informatie te verkrijgen voor kwaadaardig gebruik. Denk maar aan informatie zoals gebruikersnamen, wachtwoorden of bankgegevens.

Met URL phishing gebruiken cybercriminelen e-mail om hun slachtoffers te misleiden om gevoelige informatie in te voeren op een nepwebsite. Die website ziet eruit als een legitieme website. URL phishing staat ook bekend als: nepwebsites en phishingwebsites.

Impact van URL phishing
Bij ongeveer 32 procent van de inbreuken gaat het om phishing. Veel phishing-aanvallen bevatten kwaadaardige links naar nepwebsites. Het gebruik van URL's in phishing e-mails is populair en effectief. Helaas klikt ongeveer 4 procent van de ontvangers in een bepaalde phishing-campagne op de kwaadaardige link.

Hackers hebben maar één persoon nodig om ze binnen te laten. Gezien het succespercentage is het niet verrassend dat de gerapporteerde verliezen in 2019 als gevolg van phishing bijna $58 miljoen bereikten. Dat is slecht nieuws, aangezien slechts 57 procent van de organisaties over URL-bescherming beschikt volgens recentelijk onderzoek.

E-mailbeveiliging tegen URL phishing
Gateways zijn zeer effectief in het beschermen tegen massale URL phishing-aanvallen. Gateways gebruiken technologieën voor het filteren van URL's en het herschrijven van URL's om de toegang tot kwaadaardige websitelinks te blokkeren, die via e-mail worden verspreid, inclusief alle bekende malware- en phishing-sites. Sandboxing kan ook helpen bij het blokkeren van kwaadaardige links. API-gebaseerde inbox defense vormt een aanvulling op de beveiliging die een gateway biedt.

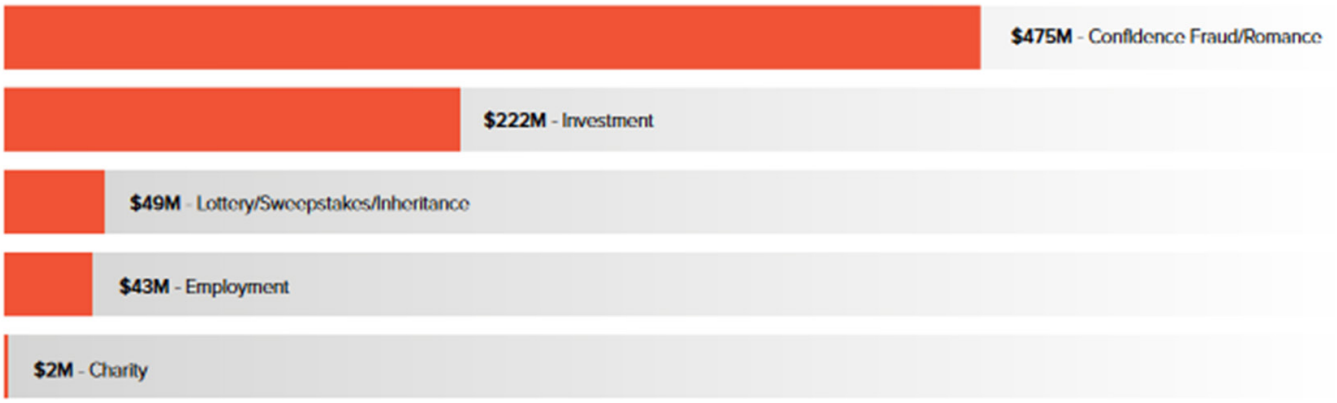
Scamming

Bij e-mail scamming gebruiken cybercriminelen frauduleuze schema's om slachtoffers te bedriegen of hun identiteit te stelen door hen te misleiden om persoonlijke informatie vrij te geven. Voorbeelden van oplichting zijn onder meer valse vacatures, investeringsmogelijkheden, kennisgevingen van overerving, loterijprijzen en geldovermakingen.

De impact van scamming
Scamming is verantwoordelijk voor 39 procent van alle spear-phishing-aanvallen. Oplichters gebruiken verschillende technieken, variërend van nep-loterijwinsten tot investeringszwendel. Het is niet ongebruikelijk dat oplichters tragedies uitbuiten, zoals orkanen, de CoVid-19-crisis en andere rampen. Oplichters jagen op de sympathie, liefdadigheid of angst van een persoon. Helaas vallen veel individuen voor oplichting via e-mail, het ongewild delen van gevoelige informatie of het doen van betalingen aan oplichters. de FBI heeft miljoenen dollars aan gerapporteerde verliezen geregistreerd als gevolg van deze oplichting.

E-mailbeveiliging tegen scamming
API-gebaseerde inbox defense bepaalt aan de hand van mailverkeer hoe de standaard e-mailcommunicatie eruitziet voor elke werknemer. Wanneer criminelen e-mails naar hun slachtoffers sturen die buiten de normale en verwachte communicatie vallen, wordt deze gemarkeerd en geblokkeerd door de inbox defense.

Gateways-oplossingen vertrouwen op gestuctureerd beleid, op zoek naar specifieke zoekwoorden die oplichting aangeven op basis van de inhoud van de e-mail. In combinatie met reputatiefilters en black lists kan dit effectief zijn. Helaas leidt dit vaak tot false positives, waardoor wordt voorkomen dat belangrijke berichten worden bezorgd in de inbox van gebruikers. Veel oplichtende e-mails kunnen ook als spam worden geclassificeerd. Organisaties moeten zowel spamfilters bij de e-mailgateway als op API gebaseerde inbox defense inzetten voor effectieve bescherming tegen oplichting.



Spear phishing

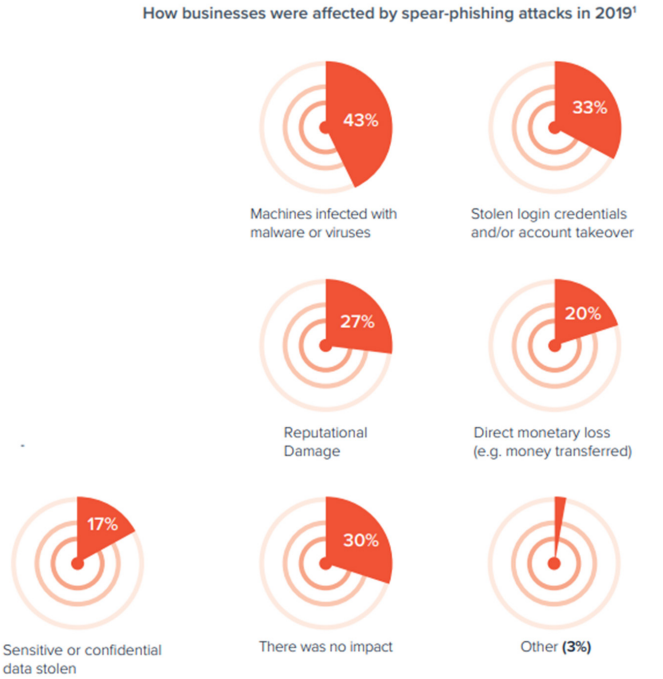
Spear phishing is een zeer gepersonaliseerde vorm van e-mail phishing-aanval. Cybercriminelen stellen zorgvuldig ontworpen berichten op, waarbij ze zich vaak voordoen als een vertrouwde collega, website of bedrijf. Spear phishing e-mails proberen doorgaans gevoelige informatie te stelen, zoals inloggegevens of financiële gegevens, die vervolgens worden gebruikt om fraude, identiteitsdiefstal en andere misdaden te plegen. Cybercriminelen profiteren ook van social engineering-tactieken in hun spear phishing-aanvallen, waaronder urgentie, beknoptheid en druk, om de kans op succes te vergroten. Spear phishing staat ook bekend als: walvisvangst en laserphishing.

Invloed van spear phishing
In de recente e-mailonderzoeken blijkt dat 43 procent van de organisaties de afgelopen 12 maanden het slachtoffer is geweest van een spear phishing- aanval. Slechts 23 procent van de organisaties zei echter dat ze speciale spear phishing bescherming hebben ingesteld.

Wanneer organisaties het slachtoffer worden van spear phishing-aanvallen, zijn er onder meer directe verliezen via overboekingen en reputatieschade. In veel gevallen leiden spear phishingaanvallen tot de diefstal van inloggegevens en de overname van e-mailaccounts. Gecompromitteerde accounts worden vaak gebruikt om een volgende spear phishing-aanval uit te voeren. Organisaties hebben speciale spear phishing bescherming nodig om deze vicieuze cirkel te stoppen.

E-mailbeveiliging tegen spear phishing
API-gebaseerde inbox defense maakt gebruik van toegang tot oude e-mail communicatiegegevens om een communicatie-identiteit op te bouwen door middel van bijvoorbeeld graph, een statistisch model dat specifiek is voor elke gebruiker in de organisatie. De identiteitsgrafiek wordt vervolgens gebruikt om ongebruikelijke communicatiepatronen te detecteren, die buiten het statistische model vallen. Deze grafiek maakt het mogelijk om spear phishing aanvallen te voorspellen en zodoende te blokkeren.

Traditionele gateways voor e-mailbeveiliging hebben geen zicht op het verledengegevens. Ze evalueren elke e-mail op basis van een set van vooraf bepaalde beleidsregels, filters en handtekeningen, in plaats van op historische communicatie en context. Spear phishing-aanvallen zijn ontworpen om deze filters en beleidsregels te omzeilen.



MX-Relay

Domein imitatie

Domein Imitatie wordt vaak door hackers gebruikt als onderdeel van een aanval om een gesprek te kapen. Aanvallers proberen een domein na te bootsen door technieken te gebruiken zoals typosquatting, het vervangen van een of meer letters in een legitiem e-maildomein door een soortgelijke letter of het toevoegen aan het legitieme e-maildomein. Ter voorbereiding op de aanval registreren cybercriminelen zich of kopen het nagebootste domein. Domeinimitatie is ook bekend als: typosquatting en lookalike domeinen.

Domeinimitatie is een aanval met een grote impact. Het komt vaak voor dat de subtiele verschillen tussen de legitieme e-mail en het nagebootste domein over het hoofd worden gezien. Wanneer bijvoorbeeld een aanvaller die blackip.nl probeert na te bootsen, zou onderstaande een zeer vergelijkbare URL kunnen zijn:

- Blackipp.nl
- Blackíp.nl
- Blackep.nl
- Blackkip.nl
- Blacip.nl

Soms verandert een aanvaller het topleveldomein (TLD), met .net of .co in plaats van .com, om slachtoffers voor de gek te houden:

- Blackip.net
- Bleckip.co

Gevolgen van domein imitatie
De afgelopen maanden hebben onderzoekers een sterke stijging gezien in domeinimitatie-aanvallen die worden gebruikt om een gesprek te kapen. Een analyse van ongeveer 500.000 maandelijkse e-mailaanvallen toont een toename van 400 procent in aanvallen op het imiteren van domeinen gebruikt voor het kapen van gesprekken.

E-mailbeveiliging tegen domein nabootsing
De grootste uitdaging wat betreft domein imitatie is het detecteren van typosquatted domeinen en het onderscheid maken tussen een nabootsing en een echte website. E-mailgateways maken lijsten van domeinen die worden gebruikt door organisatie. Een lang proces dat vatbaar is voor fouten en continu beheer en updates nodig heeft. Ondanks dat gateways domein nabootsing kunnen detecteren, zijn er zo veel emaildomeinen en variaties dat die alsnog kunnen leiden tot false positives, waardoor aanvallen door de beveiliging heen komen.

Een op API gebaseerde inbox defense maakt gebruik van eerdere e-mailcommunicatie om gegevens te krijgen over domeinen die worden gebruikt door de organisatie, hun partners, en klanten. Inbox defense koppelt specifieke gesprekken, verzoeken en personen met specifieke e-maildomeinen. Als een leverancier een ongebruikelijk verzoek stuurt vanuit het verkeerde domein, detecteert inbox defense dit en blokkeert het verzoek.

+400%

Domain impersonation increase in 2H 2019

Merk imitatie
Merk imitatie is een emailbedreiging waarbij de imitator zich voordoet als een bedrijf of merk. Dit wordt gedaan om slachtoffers te misleiden door te reageren en persoonlijke of anderszins gevoelige informatie openbaar te maken. **Veel voorkomende soorten imitatie van een merk zijn:**

Service imitatie
Deze phishing-aanval is ontworpen om zich voor te doen als een bekend bedrijf of algemeen gebruikte zakelijke applicatie. Het is een populaire vorm van phishing omdat de e-mails zijn ontworpen als een toegangspunt om inloggegevens te verzamelen en een accountovername uit te voeren. Service imitatie aanvallen worden ook gebruikt om persoonlijk identificeerbare informatie te stelen, zoals creditcard- en burgerservicenummers. Service imitatie is ook bekend als: leverancier e-mail compromis.

Merkkaping
Merkkaping is een veel voorkomende vorm van phishing. Een aanvaller wil het domein van een bedrijf gebruiken om zich uitgeven voor een bedrijf of een van zijn werknemers. Dit wordt meestal gedaan door e-mails te verzenden met valse of vervalste, domeinnamen die legitiem lijken. Merkkaping is ook bekend als merkspoofing en domein spoofing.

Impact van merk imitatie
Service imitatie wordt gebruikt bij 47 procent van alle spear phishing-aanvallen. Microsoft is het meest geïmiteerde merk in spear phishing-aanvallen. Zich voordoen als Microsoft is een van de meest voorkomende technieken die door cybercriminelen wordt gebruikt om een account over te nemen. Inloggegevens van Microsoft en Office 365 zijn van grote waarde, omdat deze hackers in staat stellen organisaties binnen te dringen en extra aanvallen te lanceren.

Brandkaping of spoofing-aanvallen worden mogelijk gemaakt door een zwakte in de e-mail RFC-standaard waarbij volledige authenticatie van verzendende domeinen niet nodig is. Standaarden zoals DKIM, SPF en DMARC maken het veel moeilijker om deze aanvallen te volbrengen. Domein-spoofing wordt echter veel gebruikt door hackers bij imitatie aanvallen. Uit een recente studie bleek dat er elke dag bijna 30.000 spoofing-aanvallen zijn. Plus, 77 procent van de Fortune 500-bedrijven heeft geen DMARC beleidsregels ingesteld, waardoor het voor oplichters gemakkelijk wordt om hun merken te kapen in phishing-aanvallen.

E-mail defense tegen merk nabootsing
Een op API gebaseerde inbox defense, ter voorkoming van persoons imitatie, gebruikt oude en interne e-mailberichten om inzicht te krijgen in mailverkeer binnen een organisatie. De gegevens worden gebruikt in een statistische detectiemodel om het verschil tussen nep en legitieme e-mails te onderscheiden, inclusief het merk en de afbeeldingen van de legitieme services die door een organisatie worden gebruikt. Gateways hebben geen zicht op de services die worden gebruikt door een organisatie en kunnen de specifieke merken en afbeeldingen niet herkennen als zijnde een legitiem merk. Ze vertrouwen op vooraf bepaald beleid, een aanpak die niet schaalbaar is gezien de verscheidenheid aan service imitatie-aanvallen.

API-gebaseerde inbox defense is effectiever bij het blokkeren van service imitatie-aanvallen. Organisaties kunnen inzicht krijgen in domeinfraude met behulp van DMARC-authenticatie ter bescherming tegen domeinvervalsing en merkkaping. DMARC-rapportage geeft inzicht in hoe een e-maildomein wordt gebruikt, wat op zijn beurt een organisatie toelaat om DMARC-handhavingsbeleid in te stellen om spoofing van het domein te voorkomen.

MX-Relay

Blackmail

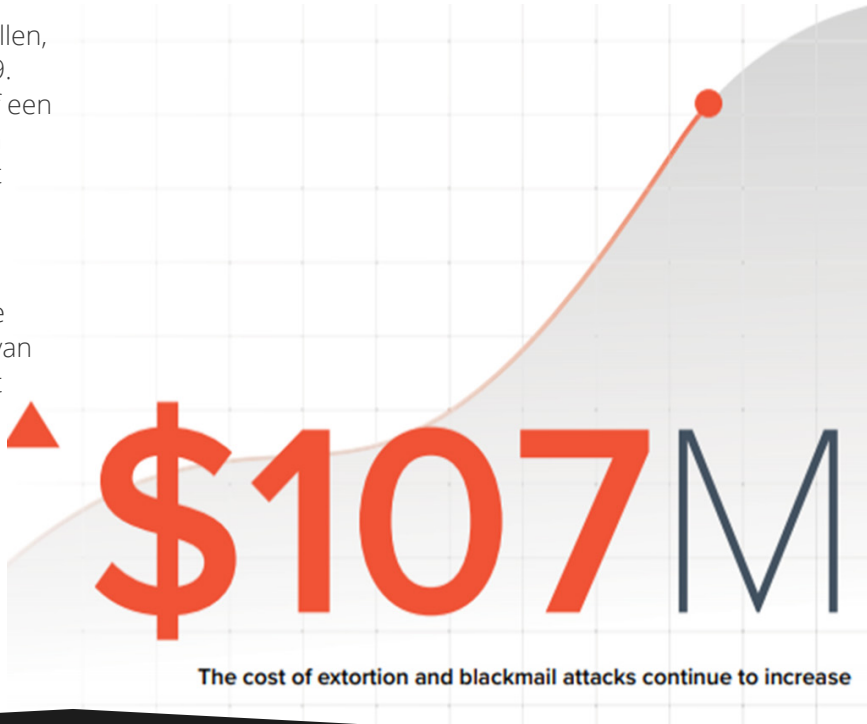
Blackmail, waaronder sextortion, wordt steeds geavanceerder, waardoor het voor e-mailgateways moeilijker wordt om deze te blokkeren. Bij sextortion-aanvallen maken cybercriminelen gebruik van gebruikersnamen en wachtwoorden welke gestolen zijn bij datalekken. Met behulp van de informatie nemen ze contact op met de slachtoffers om hen te misleiden en zodoende geld af te troggelen. De oplichters beweren dat ze een compromitterende video hebben opgenomen op de computer van het slachtoffer en dreigen deze te delen met al hun contacten, tenzij ze betalen. Chantage wordt ook wel afpersing en sextortion genoemd.

Gevolgen van Blackmail
Blackmail vormt ongeveer 7 procent van de spear phishing-aanvallen, hetzelfde percentage als het compromitteren van zakelijke e-mail. Werknemers zijn net zo waarschijnlijk het doelwit van een chantagezwendel als een aanval gericht op het bedrijf via e-mail.

Volgens de FBI zijn de kosten van afpersingsaanvallen, inclusief blackmail, meer dan $107 miljoen in 2019. Aanvallers vragen gemiddeld een paar honderd of een paar duizend dollars, een bedrag dat een persoon waarschijnlijk zou kunnen betalen. Door een groot aantal aanvallen lopen de kleine betalingen substantieel op voor aanvallers. Blackmail-scams worden te weinig gerapporteerd vanwege de opzettelijk beschamende en gevoelige aard van de bedreigingen. IT-teams zijn zich vaak niet bewust van deze aanvallen omdat werknemers de e-mails niet rapporteren, ongeacht of ze het losgeld betalen.

Versterking van e-mail defense tegen Blackmail
Inbox defense heeft toegang tot historische e-mails via API's. Het bouwt een statistisch model van communicatiepatronen, inclusief de tone of voice die door individuen wordt gebruikt. Hierdoor kan Inbox defencs de ongebruikelijke en bedreigende toon van chantage-aanvallen herkennen. In combinatie met andere signalen kunnen zodoende schadelijke e-mails worden gemarkeerd.

Gateways kunnen sommige tekenen van chantage herkennen, zoals het gebruik van bepaalde zoekwoorden. Het gebrek aan zichtbaarheid in historische e-mailgegevens en onvermogen om iets abnormaals te herkennen op basis van tone of voice weerhoudt de techniek wel om organisaties optimaal te beschermen tegen chantage-aanvallen.



Zakelijke gecompromitteerde accounts, BEC- aanvallen

Bij BEC-aanvallen (business e-mail compromise) doen oplichters zich voor als een werknemer in de organisatie om zo fraude te plegen binnen het bedrijf, zijn werknemers, klanten of partners. In de meeste gevallen concentreren aanvallers hun inspanningen op werknemers met toegang tot de financiën of persoonlijke informatie van het bedrijf. Door middel van het misleiden van personen bij het uitvoeren van elektronische overboekingen of het vrijgeven van gevoelige informatie.

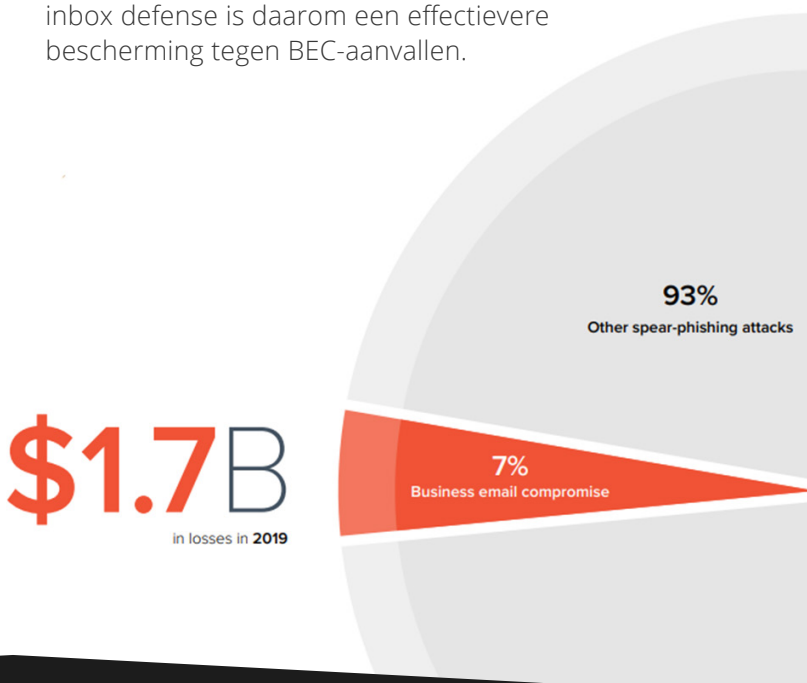
Deze aanvallen maken gebruik van social engineering tactieken en gecompromitteerde accounts. Ze bevatten vaak geen bijlagen of links. BEC is ook bekend als: CEO-fraude, CFO-fraude, nabootsing van werknemers, walvisvangst, social engineering, en fraude met overboekingen.

Inbreuk op zakelijke e-mail
Terwijl zakelijke e-mail aanvallen slechts 7 procent uitmaken van spear phishing-aanvallen veroorzaakten deze meer dan $ 1,7miljard aan verliezen alleen al in 2019, aldus de FBI. Gmail-accounts zijn gewend om 47 procent van de zakelijke e-mailaanvallen te weren.

Payroll-scams zijn een populaire vorm van BEC-aanval. Deze vorm van oplichting richt zich op human resources en payroll-afdelingen met als doel het salaris van een werknemer over te boeken naar een andere, frauduleuze account. Hackers doen zich voor als werknemers en geven nieuwe account details door voor de salarisstorting. Payroll-zwendel is goed voor 8 procent van de BEC-aanvallen. Echter nemen ze fors toe en groeien recentelijk meer dan 800 procent.

E-mail defense tegen gecompromitteerde zakelijke email
API-gebaseerde inbox defense, gebruikt e-mailgegevens en bouwen op basis daarvan een statistisch model of een identiteitsgrafiek. Dit wordt gebruikt om te begrijpen wie met elkaar communiceert en welke namen en identiteiten ze gebruiken. Het analyseert ook typische verzoeken tussen medewerkers binnen de organisatie met behulp van sentimentanalyse. Wanneer een ongebruikelijk verzoek wordt gedaan detecteert API-gebaseerde inbox defense de nabootsing van identiteit op basis van de geschiedenis van communicatie.

E-mailgateways hebben geen zicht op relaties en communicatiepatronen tussen individuen op basis van historisch gegevens. Gateways vertrouwen op aangepast gedetailleerd beleid en DMARC voor bescherming tegen spoofing en nabootsing van identiteit. Deze technieken zijn niet voldoende om te beschermen tegen BEC en leidt tot grote aantallen van false positives & negatives. API-gebaseerde inbox defense is daarom een effectievere bescherming tegen BEC-aanvallen.



Gesprek kaping

Bij het kapen van gesprekken voegen cybercriminelen zichzelf toe aan bestaande zakelijke gesprekken of starten nieuwe gesprekken op basis van de informatie die ze hebben verzameld van gecompromitteerde e-mailaccounts, om zodoende geld te of persoonlijke informatie te ontvangen.

Het kapen van een conversatie kan deel uitmaken van een accountovername-aanval. Aanvallers besteden tijd aan het lezen van e-mails en het monitoren van het gecompromitteerde account om inzicht te krijgen in het zakelijke proces van lopende deals en betaling procedures. Cybercriminelen gebruiken de gecompromitteerde accounts zelden om een gesprek te kapen. In plaats daarvan gebruiken aanvallers imitatie van e-maildomeinen.

Gevolgen van het kapen van een gesprek
De afgelopen maanden is er een sterke stijging geweest van meer dan 400 procent van domein imitatie wat gebruikt wordt voor gesprek kaping. Aanvallen zijn erg persoonlijk, waardoor ze effectief, moeilijk te detecteren en kostbaar kunnen zijn.

Versterking van e-mail defense tegen gesprekskaping
Inbox defense verleent toegang tot e-mailcommunicatie via API-integratie, waarbij die gegevens gebruikt worden om te begrijpen wie met wie zal communiceren, inclusief gebruikelijke externe contacten en interacties met hen. Wanneer een e-mail gesprek wordt gekaapt en een vertrouwde partner wordt nagebootst door cybercriminelen, blokkeert inbox defense de aanval.

Gateways hebben die zichtbaarheid niet. Deze aanpak is moeilijk schaalbaar en kan leiden tot false positives. Wanneer een gesprek wordt gekaapt, bezorgt de gateway alsnog de e-mail. De gateway beschermt niet genoeg tegen dit soort aanvallen.

Lateral Phishing

Bij lateral phishing gebruiken aanvallers recentelijk gekaapte accounts om phishingmails te verzenden aan nietsvermoedende ontvangers, zoals nauwe contacten in het bedrijf en externe partners, om de aanval breder te verspreiden. Omdat deze aanvallen afkomstig zijn van een legitieme e-mail account en lijken van een vertrouwde collega of partner te zijn, hebben ze meestal een hoog slagingspercentage.

Gevolgen van lateral phishing
Deze aanvallen, gericht op een breed scala aan slachtoffers en organisaties, kunnen extreem schadelijk zijn voor de merkreputatie van een bedrijf. Meer dan 55 procent van deze aanvallen is gericht op ontvangers, welke een werk- of persoonlijke verbinding met het gekaapte account hebben. Niet verrassend genoeg slaagt ongeveer 11 procent van deze aanvallen met succes om extra accounts te compromitteren, wat leidt tot nog meer lateral phishing-aanvallen.

Versterking van e-mail defense tegen lateral phishing
In de meeste gevallen is laterale phishing een interne aanval. E-mailgateways hebben geen zicht op deze communicatie en kunnen de aanvallen intern niet stoppen, omdat ze er nooit doorheen gaan. Gateways kunnen aanvallen ook niet herstellen voordat ze afgeleverd zijn. Zodra de e-mail is afgeleverd bij de inbox, blijft het daar. API's voor inbox defense bieden zichtbaarheid in interne communicatie. Ze kunnen interne bedreigingen detecteren, zoals laterale phishing, en herstel deze na de levering.

In een recente studie ontdekten onderzoekers dat 1 op de 7 organisaties een laterale phishing-aanval heeft gehad.

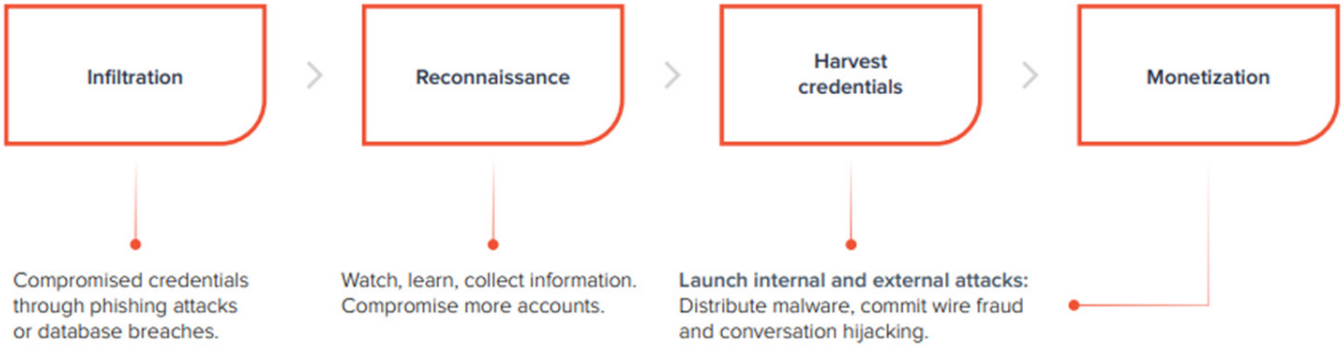
Accountovername

Accountovername is een vorm van identiteitsdiefstal en fraude, waarbij een kwaadwillende derde partij met succes toegang kan krijgen tot de accountgegevens van een gebruiker. Cybercriminelen gebruiken imitatie van het merk en phishing om inloggegevens te stelen en toegang te krijgen tot e-mailaccounts. Zodra het account is gecompromitteerd, volgen hackers de activiteiten om erachter te komen hoe het bedrijf zaken doet, de e-mailhandtekeningen die ze gebruiken en de manier waarop financiële transacties worden afgehandeld. Dit helpt hen succesvolle aanvallen te lanceren, waaronder het verzamelen van extra inloggegevens voor andere accounts. Accountovername is ook bekend als: *account compromise.*

Impact van accountovername
Uit een recente analyse van aanvallen op accountovername bleek dat in één maand, 29 procent van de organisaties een Microsoft Office 365-account had welke gecompromitteerd was door hackers. Meer dan 1,5 miljoen kwaadaardige en spam e-mails werden verzonden door de gehackte Office 365-accounts in die periode van 30 dagen.

Inbox defense tegen accountovername
Gateways bevinden zich buiten een organisatie, zodat ze zijn losgekoppeld van e-mailinboxen en gebruikers. Ze missen het vermogen om te controleren op verdacht gedrag, zoals aanmeldingen van ongebruikelijke locaties of berichten die intern worden doorgestuurd.

Een op API-gebaseerde inbox defense maakt rechtstreeks verbinding met de inbox van gebruikers, controleert op verdachte wijzigingen in inboxregels, ongebruikelijke login activiteit en kwaadaardige berichten die zijn verzonden door reeds gecompromitteerde rekeningen. Inbox defense detecteert eventuele accountovername, voordat deze wordt gebruikt om fraude uit te voeren. Inbox defense blokkeert de aanval door kwaadwillende personen te vergrendelen uit de gecompromitteerde account.



How an account takeover attack happens

Versterking van uw e-mail beveiliging met API-gebaseerd Inbox Defense

Traditionele beveiliging van e-mailgateway
De e-mailgateway is een beveiligingsysteem die voor uw mailserver is ontworpen om inkomend en uitgaand verkeer te filteren op mailberichten met schadelijke inhoud. E-mailgateways gebruiken technologieën zoals reputatiefilters om te zoeken naar IP's met een slechte reputatie. Bij afzenders van e-mail met een slechte reputatie kunnen hun verbindingen worden geweigerd of hun berichten worden teruggestuurd op basis van uw voorkeuren. Ze evalueren e-mailinhoud op tekenen van kwaadwillende bedoelingen, scannen op virussen en malware, identificeren de afzender en analyseren URL's. Tevens blokkeert de e-mailgateway alle sites die verbonden zijn tot phishing-sites of sites die hiervoor zijn ontworpen om malware verspreiden.

E-mailgateways zijn zeer effectief bij het detecteren en het blokkeren van zero-day-aanvallen en ransomware. Deze laag van bescherming omvat geavanceerde beschermingstechnologieën tegen bedreigingen, zoals sandboxing, die nieuwe, nooit eerder geziene varianten van malware in een gecontroleerde omgeving analyseert.

Gateways zijn de noodzakelijke basis voor e-mailbeveiliging. Ze blokkeren de meeste kwaadaardige berichten, inclusief spam, op grote schaal phishing-aanvallen, malware, virussen en zero-day-aanvallen. Vanwege hun extreme vertrouwen op filters, regels en beleid, zijn gateways niet voldoende om uw organisatie te beschermen van zeer gerichte e-mailaanvallen die gebruikmaken van social engineering tactieken, waaronder spear phishing en het in gevaar brengen van zakelijke e-mail.

Gateways zoeken naar tekenen van kwaadaardige inhoud of afzenders, maar ze laten aanvallen door die geen van hun vooraf bepaalde beleidsregels, filters of verificatieregels activeren.

API-gebaseerde Inbox Defense
Hoewel e-mailgateways nog steeds nodig zijn, zijn ze niet meer voldoende om u te beschermen tegen de ontwikkeling van cyberdreigingen. Om uw organisatie te beschermen tegen speciaal ontworpen aanvallen heeft u een extra verdediging laag nodig – die meer biedt dan de gateway en op inbox-niveau.

Inbox defense is afhankelijk van API's welke rechtstreeks met uw e-mailomgeving integreren, inclusief individuele inboxen. Door het gebruik van API integratie heeft u inzicht in zowel historisch als dagelijkse e-mailcommunicatie voor elk individu in de organisatie. Het maakt vervolgens gebruik van deze communicatiegegevens en kunstmatige intelligentie (AI) om voor elke gebruiker een identiteitsgrafiek te maken die hun communicatiepatronen weergeeft.

De identiteitsgrafiek is gebouwd met behulp van meerdere classificaties die bepaalt hoe normale e-mailcommunicatie er voor elk uitziet werknemer. Het analyseert bijvoorbeeld (gebaseerd op historisch gegevens) vanaf welke locaties elke medewerker waarschijnlijk zal inloggen. Tevens analyseert het emailadressen, individuen waarmee ze communiceren, het soort verzoeken dat ze doen en honderden andere signalen. Wanneer er iets abnormaals gebeurt dat buiten een identiteitsgrafiek van het individu valt, markeert AI dit als mogelijk kwaadaardig en verwijdert het uit de inbox van de gebruiker, voordat ze kunnen communiceren met het bericht.

Hoewel u e-mailgateways op een vergelijkbare manier kunt laten werken, is die oplossing niet schaalbaar. Veel van de huidige e-mailgateways zorgen dankzij gedetailleerde aanpassing en beleidsinstellingen dat gerichte aanvallen worden geblokkeerd.

Elke classificator kan mogelijk worden omgezet in een regel of beleid voor de gateway, maar met honderden beleidsregels die moeten worden opgezet voor duizenden werknemers, is het de oplossing niet schaalbaar. Het past een verandering niet aan en het is vatbaar voor een groot aantal false positives and negatives.

Organisaties vertrouwen op gateways om hun gebruikers te beschermen tegen spear phishing-aanvallen welke in staat zijn om een select aantal werknemers te beschermen die geïdentificeerd worden als hoog risico. Het is onvermijdelijk dat spear phishing-aanvallen door hun gateways gaan en in de inbox van gebruikers terecht komen.

"Upgrade naar een beveiligde e-mail gateway-oplossing om gebruik te maken van geavanceerde phishing-bescherming, identiteit vervalsing en interne e-mail bescherming."

Conclusie: Effectief beschermen tegen evoluerende e-mailbedreigingen

Email Threat Taxonomy - 13 Threat Types

THREAT TYPES	EMAIL GATEWAY	API-BASED INBOX DEFENSE
Spam	●	○
Malware	●	○
Data Exfiltration	●	○
URL Phishing	◑	●
Scamming	◑	●
Spear Phishing	○	●
Domain Impersonation	○	●
Service Impersonation	○	●
Blackmail	◑	◑
Business Email Compromise	○	●
Conversation Hijacking	○	●
Lateral Phishing	○	●
Account Takeover	○	●

○ Does not provide sufficient protection ◑ Provides some protection ● Provides best protection

Blokkeer grote aanvallen bij de gateway
Gateways zijn de noodzakelijke basis voor e-mailbeveiliging. Ze blokkeren de meeste kwaadaardige berichten, inclusief spam, grootschalige phishing-aanvallen, malware, virussen en zero-day-aanvallen. Als deze aanvallen niet worden gecontroleerd kunnen ze een binnen uw organisatie een ravage veroorzaken, met gevolgen voor de productiviteit en ze kunnen uw apparaten infecteren.

Bescherm uw gebruikers op inbox-niveau
Hoewel gateways belangrijk zijn, zijn ze niet meer voldoende op zichzelf. API gebaseerde inbox defense ontgrendelt toegang tot historische en interne e-mailcommunicatie, die nodig is om uw gebruikers te beschermen tegen zeer gerichte aanvallen die langs gateways glippen.

Leer gebruikers over de nieuwste bedreigingen
Sommige evoluerende en geavanceerde phishing-aanvallen, inclusief degenen die social-engineeringtactieken gebruiken, kunnen door de beveiligde e-mailgateway glippen. Bescherm tegen dit soort bedreigingen door middel van trainingen voor bewustzijn van werknemers. Met simulatie en training, kunnen medewerkers kwaadwillende herkennen en melden waardoor de medewerker tevens een verdedigingslaag wordt.

MX-Relay

Zorgeloze e-mailervaring met Office365 Inbox Defense en MX-Relay

MX-Relay

MX-Relay is het meest eenvoudige en betrouwbare e-mail beveiligingssysteem van het web aanbieden. Deze is gericht op de totale e-mail infrastructuur, met focus op spam & malware, fraudebescherming en bewustzijn van gebruikers en organisaties zelf.

Benieuwd wat MX-Relay voor uw organisatie kan betekenen of wilt u direct een 30 dagen trial aanvragen? Kijk dan snel op onze website!

Aan de slag met Office365 Inbox Defense

Inbox Defense detecteert bedreigingen die traditionele e-mail security gateways niet kunnen herkennen.

Het analyseert de unieke communicatiepatronen van een organisatie om afwijkingen in veel voorkomende combinaties van bijvoorbeeld afzender, ontvanger, e-mail adres te detecteren. Ook wordt de bodytekst van de e-mail geïnspecteerd op aanwijzingen die mogelijk duiden op een spearphishing aanval. Inbox Defense combineert beide methoden om te bepalen of een e-mailbericht deel uitmaakt van zo'n aanval.

Het integreert rechtstreeks met Microsoft Office 365 API's om aanvallen te detecteren die afkomstig zijn van zowel interne als externe bronnen, inclusief bedreigingen die mogelijk al in uw Postvak IN zitten.

Nieuwsgierig geworden naar onze Office365 Inbox Defense oplossing? Ga via de onderstaande button naar de website en vraag het direct aan!

WEBSITE OFFICE365 INBOX DEFENSE