Oktober 2021

Betaal geen ransom

Bescherming tegen ransomware in drie stappen

Barracuda
Your journey, secured.

Inhoudsopgave

Barracuda

Ransomware en haar evolutie

Eenvoudig gezegd is ransomware kwaadaardige software die uw gegevens versleutelt of er op een andere manier voor zorgt dat u geen toegang meer hebt tot uw eigen systemen. Vervolgens eisen de criminelen losgeld in ruil voor de decoderingssleutel. Er is uiteraard geen enkele garantie dat deze sleutel daadwerkelijk werkt en u uw gegevens terugkrijgt. Veel slachtoffers hebben wel betaald, maar kregen hun gegevens niet terug.

Vergeleken met de eenvoudige WannaCry-aanvallen van het soort 'compromitteren en versleutelen' van een paar jaar geleden, is de huidige aanpak van aanvallers geavanceerder en omvat meerdere vectoren. Een aanval begint vaak nog steeds met een spearphishing-e-mail, maar tegenwoordig worden ransomwareaanvallen niet onmiddellijk geactiveerd wanneer het doelwit op de kwaadaardige link klikt.

In plaats daarvan gebruiken cybercriminelen deze stap om de aanmeldgegevens van het slachtoffer te bemachtigen. Deze worden vervolgens gebruikt om het netwerk van de organisatie binnen te komen. Daar blijft de aanvaller hangen en evalueert bedrijfsmiddelen, servers, databases en het e-mailplatform. Deze observatiefase kan weken of zelfs maanden duren. Pas daarna gaan ze tot de daadwerkelijke aanval over. Dit is precies wat er gebeurde bij de ransomwareaanval op de Ierse gezondheidsdienst, de HSE. De aanvallers beweren dat ze al weken in het netwerk van de HSE zaten svoordat ze overgingen tot de aanval waarbij ze 700 GB aan patiëntgegevens stalen en versleutelden.

Eén reden dat u tegenwoordig meer over ransomware hoort, is dat het makkelijker is om ermee te beginnen. De benodigde technologie voor criminaliteit wordt steeds makkelijker te gebruiken. Iemand kan nu een ransomwarekit kopen en een doelwit kiezen. De bendes bieden technische ondersteuning in ruil voor een percentage van het losgeld. Als dat toch een beetje te ver gaat, kan de aspirant-crimineel cybercriminelen inhuren om de aanval uit te voeren, als een soort cybercrime-as-a-service. Cryptovaluta wordt steeds meer waard en de populariteit van cyberverzekeringen maakt ransomwareaanvallen ook winstgevender voor cybercriminelen. Dit trekt goed georganiseerde bendes aan. Er zijn ook ransomwareaanvallen die door overheden worden gesteund, wat de zogenoemde digitale oorlogvoering naar een hoger niveau heeft getild.

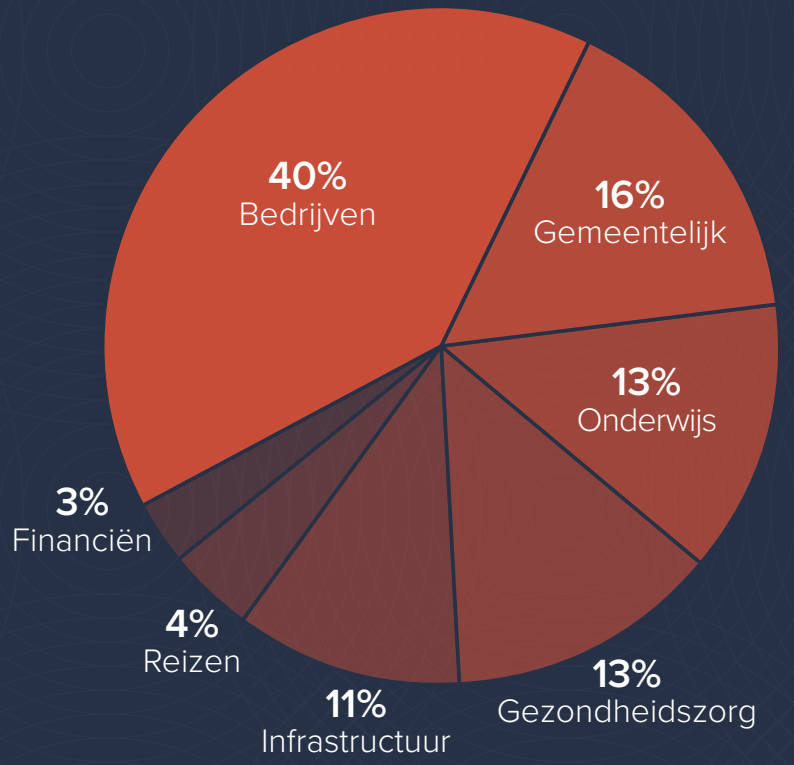
Cybercriminelen nemen de volgende stap

Ransomwareaanvallen zijn nu zo'n groot probleem dat overheden ze inmiddels beschouwen als een vorm van terrorisme. Dit is geen overdreven reactie. De aanvallen veroorzaken ingrijpende operationele storingen bij lokale overheden, wetshandhaving, onderwijsinstellingen, gezondheidszorgnetwerken, essentiële infrastructuur en meer. Geen enkele branche, organisatie of overheidsentiteit is immuun voor deze aanvallen.

Volgens recent onderzoek van Barracuda vormden aanvallen op bedrijven in sectoren zoals infrastructuur, reizen, financiële dienstverlening en meer tussen augustus 2020 en juli 2021 in totaal 57% van alle ransomwareaanvallen, een stijging ten opzichte van 18% in ons onderzoek in 2020. Infrastructuurgerelateerde bedrijven waren doelwit van 11% van de aanvallen die we onderzochten.

De losgeldbedragen worden ook steeds hoger. Gemiddeld wordt er per incident nu meer dan 10 miljoen dollar aan losgeld geëist. Volgens onderzoek van Barracuda was bij slechts 18% van de incidenten tussen augustus 2020 en juli 2021 de losgeldeis lager dan 10 miljoen dollar; bij 30% van de incidenten was deze hoger dan 30 miljoen dollar.

Ransomwareaanvallen per branche



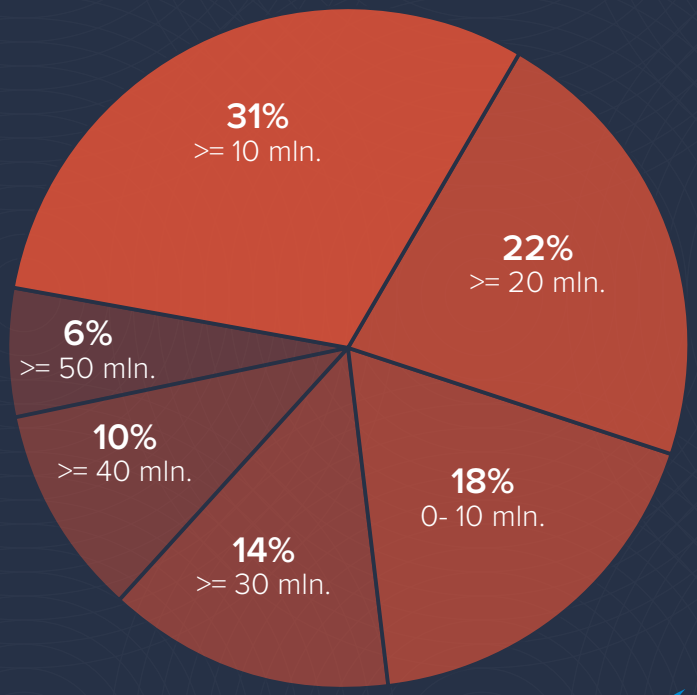
Ransomware is geen nieuwe bedreiging, maar heeft zich ontwikkeld tot een nog destructiever monster. Criminelen hebben hun vaardigheden verder ontwikkeld en hun tactieken verfijnd tot een dubbele afpersingsconstructie. Ze baseren hun losgeldeisen op onderzoek dat ze voor de aanval uitvoeren. Vervolgens stelen ze gevoelige informatie van hun slachtoffers en eisen ze een betaling in ruil voor de belofte dat deze informatie niet openbaar zal worden gemaakt of aan andere criminelen zal worden verkocht. Omdat criminelen niet te vertrouwen zijn, worden slachtoffers die betalen vaak na enkele maanden weer gecontacteerd en opnieuw om een betaling gevraagd om de gestolen gegevens geheim te houden. Sommige ransomwarecriminelen nemen het geld aan, maar verkopen de gestolen gegevens daarna alsnog.

Het is nooit gegarandeerd dat u alle versleutelde gegevens terugkrijgt als u het losgeld betaalt. Slachtoffers moeten nu begrijpen dat alle bij een ransomwareaanval gestolen gegevens voorgoed zijn gecompromitteerd. Er is geen enkele reden om criminelen te betalen voor hun misdaden.

Ga ervan uit dat uw bedrijf het doelwit zal zijn van ransomwareaanvallen. Als zo'n aanval slaagt, moet u een plan hebben waarbij u geen losgeld betaalt.

De sleutel tot het beschermen van uw bedrijf tegen ransomwareaanvallen is het beschermen van uw gegevens. Dit is onder te verdelen in drie aandachtsgebieden: uw aanmeldgegevens beschermen, uw web applicaties beveiligen en een back-up maken van uw gegevens. Laten we elk van deze stappen nader bekijken.

Losgeldeisen bij ransomware



Barracuda

Stap 1: bescherm uw aanmeldgegevens

Om te beginnen is ransomware afhankelijk van een inbreuk op e-mail of een andere manier om aanmeldgegevens te bemachtigen. Aangezien duizenden gebruikersnamen en wachtwoorden online staan, kan deze eerste stap schrikbarend makkelijk zijn. Vervolgens gebruiken aanvallers deze gestolen aanmeldgegevens om toegang te krijgen tot uw systemen.

Barracuda

Aangezien phishing de primaire aanvalsvector voor ransomware is, moet u een cultuur van bewustzijn over de beveiliging van aanmeldgegevens stimuleren. Ontwikkel een proces om gebruikers te trainen in e-mailbeveiliging en implementeer antiphishingtechnologie e implementando una tecnologia anti-phishing die ongebruikelijke activiteit kan identificeren en uitlichten. Als de aanvaller geen aanmeldgegevens kan bemachtigen, is het veel moeilijker om de aanval te escaleren van phishing naar ransomware.

Phishingaanvallen zijn effectief omdat mensen graag op iets klikken. Hackers passen hun aanvallen zorgvuldig aan op de slachtoffers door publiekelijk beschikbare persoonlijke informatie over hen te verzamelen en in te spelen op een gevoel van urgentie om een reactie te krijgen. De aanvallers hoeven slechts één persoon binnen uw organisatie ertoe te verleiden op de link te klikken of een bijlage te openen. Uit recent onderzoek van Barracuda blijkt dat gemiddeld 3% van de mensen die een phishing-e-mail ontvangen, op de link klikt. Vaak is het doel van de aanval om aanmeldgegevens te bemachtigen. Daarmee kan de hacker zich lateraal door het bedrijf verplaatsen en op de hele organisatie een ransomwareaanval uitvoeren.

Er zijn twee kanten aan het beschermen van aanmeldgegevens en toegang: eerst moet u investeren in detectie- en reactietools en daarnaast moet u zich richten op het trainen van uw gebruikers.

2,94%
KLIKT OP DE LINK IN EEN KWAADAARDIGE E-MAIL

0,78%
STUURT KWAADAARDIGE E-MAILS DOOR

0,17%
BEANTWOORDT DE KWAADAARDIGE E-MAIL

Bron: Threat Spotlight: Post-delivery email threats

Detectie- en reactietools

Het is niet voldoende als uw e-mailbeschermingstechnologie zich richt op de detectie van kwaadaardige nettoladingen die via links of bijlagen worden geleverd. Deze moet ook kunnen herkennen wanneer aanvallen gebruikmaken van social engineeringtactieken die zijn ontworpen om filtertechnologie te omzeilen en gebruikers ergens toe te verleiden. De technologie moet een e-mail controleren op kwaadaardige bedoelingen, zelfs wanneer deze geen kwaadaardige nettolading bevat. E-mailbeveiliging die gebruikmaakt van machine learningalgoritmen kan social engineeringaanvallen nauwkeuriger detecteren door te zoeken naar de kleinste afwijkingen van normale communicatiepatronen.

U kunt de aanmeldgegevens van uw gebruikers niet beschermen zonder de juiste bescherming tegen accountovername. Multifactorauthenticatie (MFA) is nog altijd een beste werkwijze. Tegenwoordig zouden alle organisaties ervan gebruik moeten maken. Het is echter geen wondermiddel en het is niet altijd genoeg. Aanvallers proberen MFA te omzeilen door gebruikers ertoe te verleiden malware op hun verificatieapparaten te installeren of nep-apps toegang te geven tot hun accounts.

Organisaties moeten bescherming tegen accountovername hebben waarbij kwaadaardige activiteit, zoals verdachte aanmeldingen of aanvallen afkomstig van gecompromitteerde accounts, snel wordt geïdentificeerd en er melding van wordt gemaakt.

Er zijn twee kanten aan het beschermen van aanmeldgegevens en toegang: eerst moet u investeren in detectie- en responstools en daarnaast moet u zich richten op het trainen van uw gebruikers.

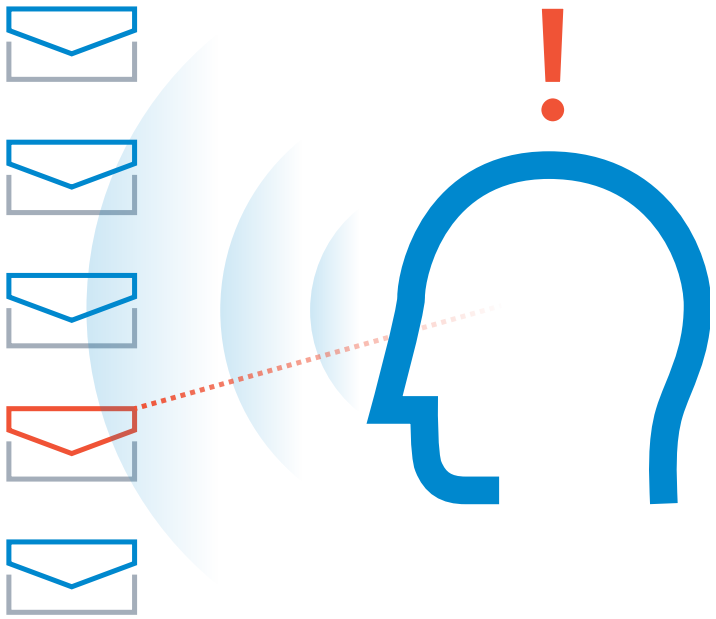
Barracuda

Uw gebruikers trainen

Uw werknemers zijn uw laatste verdedigingslinie, dus het is essentieel dat u hen traint in het herkennen en melden van aanvallen. Maak beveiligingsbewustzijnstraining en phishingsimulatie onderdeel van uw e-mailbeveiligingsstrategie. Van oudsher worden phishingaanvallen alleen met e-mail geassocieerd, maar tegenwoordig gebruiken cybercriminelen ook andere kanalen, zoals spraak- en sms-berichten. Gebruik phishingsimulatie voor e-mail, voicemail en sms-berichten om gebruikers te trainen in het identificeren van cyberaanvallen, de effectiviteit van uw training te testen en de gebruikers te evalueren die het meest kwetsbaar zijn voor aanvallen.

Zorg ervoor dat cyberbeveiligingstraining niet alleen langskomt op de eerste dag van nieuwe medewerkers. De training moet op doorlopende basis zijn om up-to-date te blijven met evoluerende bedreigingen. De bendes van vandaag maken bijvoorbeeld gebruik van geavanceerde social engineering die lastig te herkennen is. Spearphishingaanvallen richten zich op één individu of een onderdeel van één afdeling, zoals de financiële afdeling, met berichten die heel precies op het slachtoffer zijn aangepast.

Het is heel belangrijk dat de training het vertrouwen wint van de medewerkers, zodat ze alarm slaan zelfs als het om een fout gaat die ze zelf per ongeluk hebben veroorzaakt. Mogelijk is er bijscholing nodig, maar straf medewerkers niet als ze een melding doen. Veel aanvallen worden niet gemeld omdat medewerkers bang zijn dat ze de schuld krijgen, omdat ze op een link hebben geklikt of een bijlage hebben geopend. Vroege waarschuwingen zijn enorm belangrijk en verdienen lof.



Stap 2: beveilig uw web applicaties en toegang

Door de verschuiving naar werk op afstand bevinden steeds meer applicaties zich buiten het datacentrum en op internet. Soms moest er zo haastig worden omgeschakeld om de bedrijfsservices actief te houden dat de beveiliging achterbleef en criminelen staan klaar om dergelijke kwetsbaarheden te exploiteren

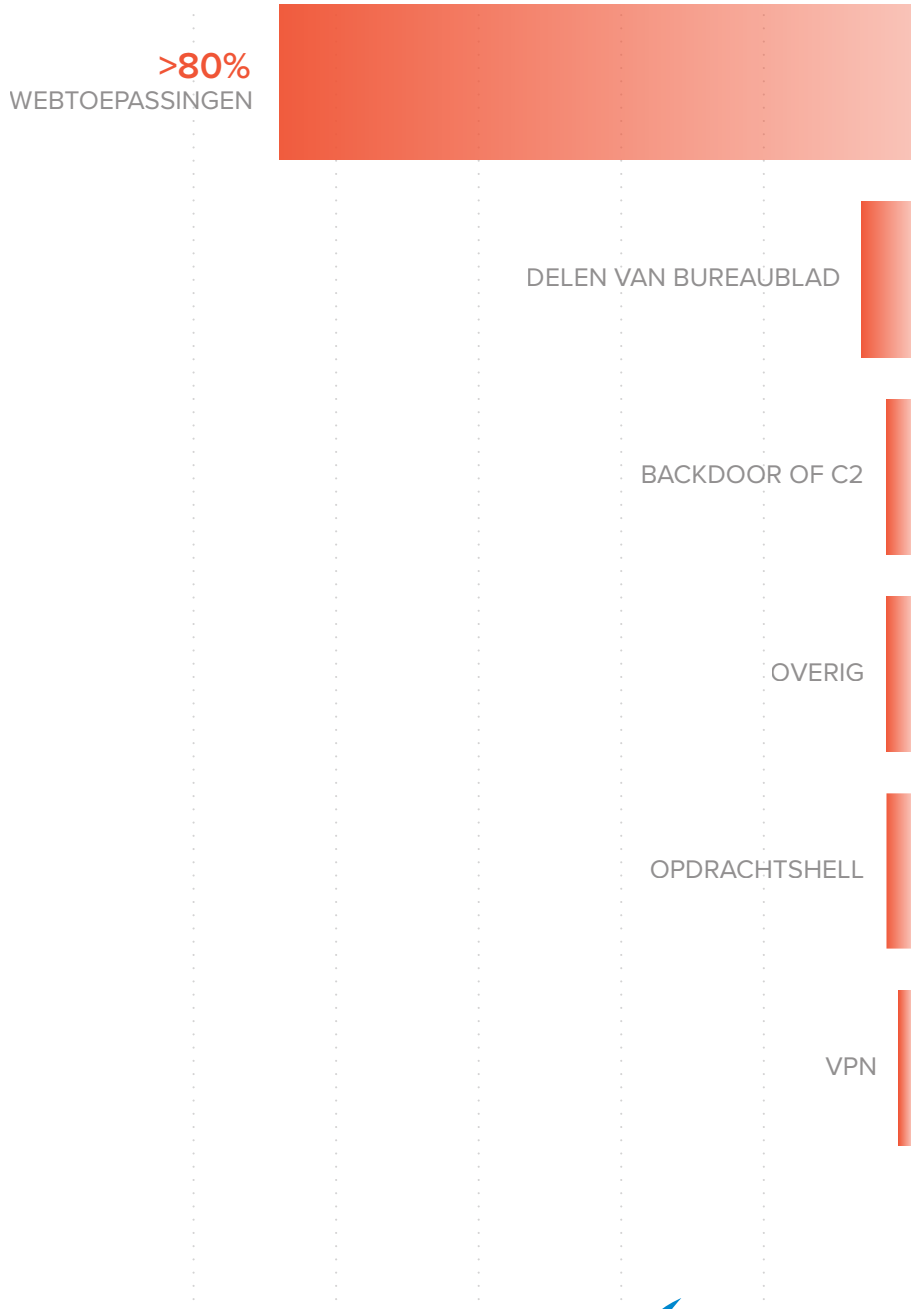
Barracuda

Uit het Verizon 2021 Data Breach Investigations Report blijkt dat web applicaties de grootste aanvalsvector in gebruik zijn voor hacking. Ze zijn goed voor meer dan 80% van alle datalekken.

Online applicaties zoals services voor het delen van bestanden, webformulieren en e-commercewebsites kunnen door aanvallers worden gecompromitteerd. Web applicaties worden via de gebruikersinterface of een API-interface aangevallen. Vaak omvatten deze aanvallen 'stuffing' van aanmeldgegevens, bruteforceaanvallen of OWASP-kwetsbaarheden. Wanneer een applicatie is gecompromitteerd, kan de aanvaller ransomware en andere malware in het systeem introduceren. Daarna verplaatst de aanvaller zich lateraal door de toepassing en kan zowel uw netwerk als dat van de gebruikers geïnfecteerd worden.

Het is belangrijk om te begrijpen dat het net zo essentieel is om toepassingen en toegang te beschermen als e-mailbeveiliging als het gaat om een goede verdediging tegen ransomware en andere malware. Het Open Web Application Security Project (OWASP) zet zich in om het algemeen bewustzijn van de meestvoorkomende applicatie-kwetsbaarheden die bij een ransomwareaanval kunnen worden geëxploiteerd te bevorderen.

Bron: Verizon 2021 Data Breach Investigations Report



Een recent voorbeeld is de ransomwarehack van de toeleveringsketen van REvil die in juli 2021 bekend werd gemaakt. Kwetsbaarheden in een publieksgerichte MSP-internettoepassing werden geëxploiteerd om ransomware naar de klanten te verspreiden. Doordat de applicatie diepe machtigingen had, kon de ransomware zich makkelijk verspreiden en tegen de tijd dat deze werd gestopt, was de impact al groot. Dit type hack kan in al uw internetgerichte toepassingen plaatsvinden. Aanvallers hacken de toepassing en verplaatsen zich lateraal om schade aan te brengen. Iets soortgelijks kan plaatsvinden als u uw RDP-systemen blootstelt aan internet, zelfs als u de standaardpoort wijzigt. Aanvallers gebruiken buitgemaakte aanmeldgegevens tegen deze RDP-systemen in een poging om het hele netwerk via deze onbeschermde aanvalsvector met malware te infecteren.

Tot

1500

bedrijven getroffen door de aanval op de toeleveringsketen van REvil

Barracuda.

Vier aanvalsvectoren voor web applicaties

Applicaties zijn nu een primair doelwit voor ransomware, dus zijn er vier aanvalsvectoren die u moet beschermen: toegang tot appliciaties, kwetsbaarheden in web applicaties, toegang tot infrastructuur en laterale verplaatsing.

1. Toegang tot applicaties

Stel uzelf de volgende vragen om te bepalen of de toegang tot toepassingen van uw organisaties kan worden gecompromitteerd.

- **Gebruiken uw externe of contractwerknemers onbeheerde apparaten of maken ze gebruik van Bring Your Own Device (BYOD)?** Mobiele apparaten komen het meest voor. Een onbeheerd of BYOD-apparaat kan worden gecompromitteerd en vervolgens worden gebruikt om aanmeldgegevens buit te maken of uw toepassing verder aan te vallen.
- **Hebt u zicht op alle gebruikers en apparaten binnen het netwerk?** U moet bijvoorbeeld weten wie verbinding maakt met uw gastnetwerk en of het juist is gesegmenteerd.
- **Hebt u een auditspoor voor wie wat wanneer opent?** U moet kunnen opzoeken wie toegang tot uw toepassingen krijgt, hoe ze deze openen en of ze over de juiste machtigingen beschikken.

Als een apparaat dat niet op uw netwerk thuishoort met uw netwerk wordt verbonden en iemand er hacktools op heeft gezet, is dat een ernstig probleem. Als u bovendien geen zicht op dit allemaal heeft, is het moeilijk te identificeren wie wat opent en waar de kwetsbaarheid zit, en kunt u de kwetsbaarheid niet oplossen of de toegang voor de aanvaller niet blokkeren.

2. Kwetsbaarheden in web applicaties

Kwetsbaarheden in web applicaties zijn de volgende aanvalsvector, aan de hand waarvan u bepaalt hoe goed uw toepassingen nou echt zijn beveiligd.

Stel uzelf de volgende vragen:

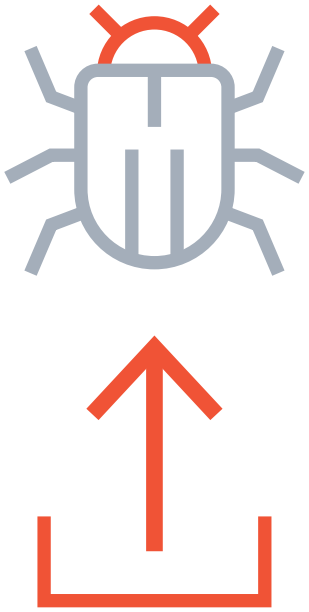
- Hoe goed is uw website beveiligd? Wanneer is deze voor het laatst bijgewerkt?
- Hebt u formulieren op uw website? Hoe voorkomt u aanvallen via formulieren?
- Accepteert u bestandsuploads op uw website? Hoe beveiligt u tegen malware?

HTTPS aanzetten is niet genoeg om uw website te beveiligen. Dat betekent alleen dat een aanvaller niet met iemand die zich op uw website aanmeldt kan meekijken om zijn of haar aanmeldgegevens te stelen. Cybercriminelen kunnen nog steeds bruteforceaanvallen uitvoeren binnen dat HTTPS-kader om juiste aanmeldgegevens voor uw website te achterhalen.

Een CAPTCHA of reCAPTCHA voor de aanmeldformulieren op uw website is ook niet voldoende, want anderen kunnen deze makkelijk automatiseren en zo deze services omzeilen.

Ook het aantal aanmeldpogingen of IP's beperken is een beveiligingsmaatregel die hackers makkelijk kunnen omzeilen met langzame aanvallen en verschillende automatiseringssystemen.

Als u bestandsuploads accepteert, is dat nog een probleem om aan te pakken. Het komt geregeld voor dat aanvallers op een website proberen in te breken door een virus of ransomware/malware te uploaden.



3. Toegang tot infrastructuur

Sinds het begin van de COVID-19-pandemie maken veel organisaties gebruik van VPN om toegang te verlenen tot intern gehoste toepassingen. Dit gebeurt wanneer er geen SaaS-vervangingen zijn voor bepaald zelfgehoste toepassingen. VPN-toegang vanuit huis bieden is dan de enige manier om het bedrijf gaande te houden. Zonder de juiste identiteits- en toegangspraktijken is dit echter een tikkende tijdbom. Veel al gestolen aanmeldgegevens gebruiken dezelfde gebruikersnamen en wachtwoorden voor toegang tot de infrastructuur. Dit vormt een ernstig risico en kan uw netwerk, toepassingen en gegevens blootstellen.

4. Laterale verplaatsingen

Nadat ze uw toepassing of infrastructuur met gestolen aanmeldgegevens hebben gecompromitteerd, proberen aanvallers uw netwerk dieper binnen te dringen en zo verder aan te vallen. Dit is dan ook de vierde aanvalsvector die u moet aanpakken. Stel uzelf de volgende vragen:

- Is uw bedrijfsnetwerk verdeeld in goed beveiligde segmenten?
- Hebt u multifactorauthenticatie ingeschakeld voor de netwerktoegang?

Het kost veel tijd en moeite om uw netwerk juist te segmenteren en u kunt uzelf er makkelijk van overtuigen om twee segmenten te openen en onderlinge toegang mogelijk te maken. Uiteindelijk leidt dit tot ongewenste toegangsmogelijkheden.

Multifactorauthenticatie voegt een belangrijke beschermingslaag toe die aanvallers de toegang tot het netwerk ontneemt.

Barracuda

Hoe een ransomwareaanval de kwetsbaarheden van toepassingen exploiteert

Hier is nog een scenario: een fictieve maar realistische serie stappen die een aanvaller kan nemen om gebrekkige toepassingsbeveiliging te exploiteren en zo een succesvolle ransomwareaanval uit te voeren. De aanval omvat een veelvoorkomende vorm van oplichting door middel van korting, die gebruikmaakt van de nieuwe golf browserplug-ins voor kortingsbonnen.

Stap 1

De aanvaller maakt een website die eruitziet als een legitieme website voor kortingsbonnen. De aanvaller doet zich voor als een website voor kortingsbonnen, wat vrij makkelijk kan via nabootsing van het domein en geautomatiseerde web-harvesting. Laten we deze nepwebsite Website X noemen.

Stap 2

De aanvaller test op een of meer van de top 10 OWASP-kwetsbaarheden om aanmeldgegevens te stelen van een legitieme maar slecht beveiligde bedrijfswebsite, die we Website Y zullen noemen. Met kwetsbaarheden zoals gebroken authenticatie en blootstelling van gevoelige gegevens kan de hacker aanmeldgegevens van gebruikers en andere gevoelige informatie buitmaken van Website Y.

Stap 3

De aanvaller lanceert met de gestolen aanmeldgegevens een 'stuffing'-aanval tegen een legitieme e-commercewebsite, die we Website Z zullen noemen. Dit is een geautomatiseerde aanval die langzaam gedurende meerdere weken kan worden uitgevoerd. Bij deze aanval is het doel om overeenkomsten te vinden tussen de gestolen aanmeldgegevens en echte accounts op deze website.

Stap 4

Als bij de aanval een overeenkomst wordt gevonden en de hacker zich kan aanmelden op het account van een slachtoffer, is de volgende stap het plaatsen van recensies van populaire producten op Website Z. Vaak is dit iets als: 'Dit product is geweldig! Klik hier voor een kortingsbon waarmee je 50% korting krijgt.' Deze link voor de kortingsbon leidt naar Website X, de nepwebsite uit stap 1.

Barracuda

Stap 5

De potentiële slachtoffers melden zich aan op Website Z en klikken op de link in de productrecensie, waarna ze naar Website X worden geleid. Ze weten niet dat ze naar een oplichtingswebsite zijn gegaan, tenzij ze heel goed naar de domeinnaam, URL, het websitecertificaat en andere details kijken. Slachtoffers die de website vertrouwen, geven vervolgens hun contactgegevens in ruil voor de kortingsbon af. De aanvaller heeft nu het adres van iemand die een e-mail van de website verwacht. De aanvaller wint het vertrouwen van het slachtoffer en het slachtoffer wordt minder waakzaam.

Stap 6

Het slachtoffer ontvangt een gepersonaliseerde e-mail over het product en de kortingsbon, met een bijlage die het slachtoffer zogenaamd moet installeren voordat de kortingsbon werkt. Deze bijlage kan een uitvoerbaar bestand zijn of een browserextensie die via JavaScript de aanval uitvoert. Omdat deze e-mail geheel is aangepast en door de ontvanger wordt verwacht, is het waarschijnlijk dat deze niet wordt tegengehouden door de traditionele e-mailbeveiliging. Het besturingssysteem van het slachtoffer waarschuwt wel om geen niet-vertrouwde uitvoerbare bestanden te installeren, maar op dit punt is het slachtoffer waarschijnlijk vol vertrouwen en klikt door.

Stap 7

Het slachtoffer installeert de bijlage en de ransomwareaanval gaat van start. Er kunnen meerdere typen aanvallen worden uitgevoerd als er eenmaal een uitvoerbaar bestand is geïnstalleerd. Zo kan bijvoorbeeld de masterbootrecord worden geïnfecteerd, kan de bestandssysteemtabel worden versleuteld en kan zelfs het opstarten van het besturingssysteem worden geblokkeerd. Kort daarna ontvangt het slachtoffer de losgeldeis. De aanvaller probeert vaak de aanval uit te breiden en meer aanmeldgegevens en andere gegevens op het netwerk te bemachtigen. Daarna versleutelt de ransomware de netwerkgegevens.

In dit voorbeeld kon de ransomware alleen slagen omdat de kwetsbaarheden in toepassingsbeveiliging op meerdere websites het overtuigende scenario lieten gebeuren: de web-harvesting van een legitieme website in stap 1, de gestolen aanmeldgegevens in stap 2, de ‘stuffing’ van aanmeldgegevens in stap 3, de oplichting via reacties en kwaadaardige URL’s in stap 4 en 5 en de installatie van het uitvoerbare bestand in stap 7. Bij elk van deze stappen had een goede apparaatbeveiliging de aanval kunnen voorkomen.

Uw applicaties en toegang beveiligen

Uw netwerk beveiligen

Voorkom dat ransomware zich in uw netwerk kan verspreiden met netwerksegmentatie en inbraakpreventie. Zoek een firewalloplossingvan de volgende generatie die:

- Meerlaagse beveiliging biedt die geavanceerde bedreigingen blokkeert, waaronder zero-dayaanvallen.
- Inbraakpreventie en sandboxing van malware omvat.
- Krachtige netwerksegmentatie biedt om laterale verplaatsing binnen het netwerk te voorkomen.

De toegang tot uw applicaties beveiligen

Beveilig de toegang tot uw toepassing met de oplossing Zero Trust Network Access (ZTNA). Deze biedt beveiligde toegang tot toepassingen en workloads vanaf elk apparaat en elke locatie.

Zoek een oplossing die:

- Voortdurend verifieert dat alleen de juiste persoon met het juiste apparaat toegang heeft tot bedrijfsbronnen.
- Toegangsbeheer op basis van rollen en kenmerken afdwingt om alleen strikt noodzakelijke toegang te geven.

ZTNA blokkeert ongeautoriseerde toegang om te voorkomen dat aanvallers inbreken op uw applicatie en ransomware verspreiden.

Barracuda

Uw web applicaties beveiligen

Een van de beste manieren om applicatie-beveiliging te implementeren is om uw software, gebruikers en hun gegevens te beschermen met een firewall voor web applicaties (WAF), waar ze zich ook bevinden. Hiermee worden botaanvallen en aanvallen waarmee services worden geblokkeerd tegengehouden en krijgt u meer inzicht in wat er gebeurt. Zoek een oplossing met de volgende kenmerken:

Makkelijk te implementeren en aan te passen aan uw omgeving

Een WAF kan u niet volledig beschermen als u deze niet kunt configureren voor uw omgeving.

Schaalbaar

Door bedrijfsgroei, digitale transformatie en andere factoren kunnen uw toepassingen en websites meer worden belast. Uw WAF moet zo nodig met uw bedrijf kunnen meegroeien.

Uitgebreide bescherming tegen geavanceerde bedreigingen

Een goede WAF biedt ten minste bescherming tegen de top 10 van OWASP en bescherming tegen DDoS op de toepassingslaag. Zoek voor volledige bescherming een oplossing die beschermt tegen zero-dayaanvallen, ‘stuffing’ van aanmeldgegevens, datalekken, kwaadaardige bots en meer.

Makkelijk bij te werken

Een WAF moet regelmatige firmware-updates hebben om de beveiliging en functies van het apparaat te verbeteren. Ideaal is een gehoste oplossing die automatisch wordt bijgewerkt zonder dat de beheerder iets hoeft te doen.

Voortdurende informatie over bedreigingen

Er worden dagelijks nieuwe aanvallen ontwikkeld en ze kunnen zich binnen enkele uren over de hele wereld verspreiden. Uw WAF moet in realtime updates ontvangen over deze aanvallen en zich aan de hand van machine learning aan varianten aanpassen.

Een goede firewall voor web appliciaties voorkomt dat ransomware zich in uw systemen nestelt door veelvoorkomende kwetsbaarheden in webtoepassingen en zero-daybedreigingen te blokkeren.

Barracuda.

Stap 3: maak een back-up van uw gegevens

Een goede verdedigingsstrategie voor ransomware kan niet zonder back-ups en noodherstel. Helaas weten criminelen dit net zo goed.

Tijdens hun ‘observatieperiode’ in het netwerk richten aanvallers zich onder andere op back-upoplossingen. Vooral de beheerconsole voor back-ups is belangrijk voor hen, omdat ze daarmee toegang krijgen tot back-upschema’s en -configuratie, retentiebeleid en de mogelijkheid om materiaal te verwijderen.

Barracuda

Aanvallers richten zich ook op de back-upopslag zelf in de hoop om uw primaire back-upserver en eventuele secundaire back-upkopieën voor noodherstel te verwijderen. Als ze eenmaal over Active Directory-wachtwoorden beschikken zodat niemand bij zijn of haar account kan, kunnen ze echt tot de aanval overgaan. Nu hebben zij de controle.

Er wordt ook nog maar al te vaak gedacht dat als uw gegevens in de cloud zijn opgeslagen, ze niet kunnen worden beïnvloed door ransomware. Dat is onjuist.

Een kind dat op de schooltablet of op zijn of haar laptop thuis op internet surft, kan bijvoorbeeld makkelijk worden verleid om op een kwaadaardige link te klikken. Als dat apparaat is verbonden en gesynchroniseerd met OneDrive als onderdeel van het Office 365-account van de school, kan een ransomwarebestand per ongeluk worden geüpload naar OneDrive en de bestanden en gegevens van de school in de Microsoft-cloud versleutelen.

Beschouw noodherstel als een essentieel, strategisch onderdeel van uw infrastructuur. Test het regelmatig en realistisch, oftewel: test het daadwerkelijke herstel, niet alleen of de functie aanstaat.

Barracuda.

We kennen ook voorbeelden waarbij SharePoint, Exchange en andere gegevensbronnen zijn getroffen. Als netwerkschijven met de functie ‘Openen met Explorer’ aan documentbibliotheken in Office 365 zijn gekoppeld, kan de ransomware bovendien scannen op bestanden op verbonden apparaten en deze infecteren.

Zelfs cloud- en SaaS-gegevens kunnen worden versleuteld door ransomware. Microsoft garandeert de beschikbaarheid van de service, maar raadt aan dat u een back-up maakt van uw gegevens met een externe back-upoplossing. Uw gegevens zijn wel opgeslagen in Microsoft Office 365, maar Office 365 is niet ontworpen om hele exemplaren na een ransomwareaanval te herstellen.

Daarom moet u back-upgegevens op de juiste manier beschermen en isoleren. Bedenk hoe vaak een systeem moet worden gespiegeld en hoe snel iemand systemen weer kan opbouwen aan de hand van die images.

U moet ervoor zorgen dat uw systemen tijdig kunnen worden hersteld via back-upversies, met gegevens die niet al te verouderd zijn. Dat betekent dat u actief actie moet ondernemen. Het is niet voldoende om in de logbestanden te controleren of gegevens vaak genoeg en nauwkeurig genoeg worden gekopieerd.

U moet echte oefeningen uitvoeren om u ervan te verzekeren dat de systemen werken. U kunt één afdeling of zelfs slechts één toepassing kiezen in plaats van alles te onderbreken. Het is echter essentieel dat u zeker weet dat u systemen tijdig kunt herstellen.

Dit is uw laatste vangnet. Zelfs als niets anders heeft gewerkt, kunnen de criminelen u niet stoppen als u een echt actuele en beveiligde back-up hebt.

Beschouw noodherstel als een essentieel, strategisch onderdeel van uw infrastructuur. Test het regelmatig en realistisch, oftewel: test het daadwerkelijke herstel, niet alleen of de functie aanstaat.

Benodigdheden voor uw back-upoplossing

Als u de risico's van ransomware wilt beperken, hebt u een uitgebreide back-upoplossing nodig met het volgende:

Onveranderbare opslag

Zelfs als de aanvaller toegang krijgt tot uw back-ups, kan hij of zij deze gegevens niet bewerken of verwijderen.

Afgesloten cloud

Bewaar een kopie van uw back-up in een beveiligde cloud op een geïsoleerd netwerk.

Multifactorauthenticatie (MFA)

Beveilig de accounts en aanmeldgegevens waarmee u toegang hebt tot de back-up.

Redundantie

Kopieer uw lokale en cloudback-ups naar een andere locatie.

Toegangsbeheer op basis van rollen

Volg het principe van strikt noodzakelijke toegang voor alle gebruikers die toegang hebben tot het back-upsysteem.

Conclusie

Mogelijk heeft uw bedrijf cyberverzekering of andere bronnen om losgeld te betalen, maar u kunt er absoluut niet van uitgaan dat u daarmee uw gegevens terugkrijgt. Er is geen enkele garantie dat hackers gegevens ontsleutelen wanneer het losgeld wordt betaald en zelfs dan toont recent onderzoek dat 80% van de organisaties die losgeld hebben betaald, opnieuw werd aangevallen.

Zelfs als u al het bovenstaande hebt gedaan, wordt u ooit aangevallen. Zelfs met de beste beveiliging is het verstandig om u voor te bereiden op het ergste. Criminelen kunnen miljoenen investeren om in uw systemen in te breken. U kunt het best maar aannemen dat ze daar ooit in slagen.

- [ ] Wie behoort tot het responsteam voor ransomware?
- [ ] Wie wordt opgeroepen als er iets in het weekend of op een feest- of vakantiedag gebeurt?
- [ ] Wie heeft de leiding?
- [ ] Wanneer stelt u uw klanten en leveranciers op de hoogte?
- [ ] Wie levert juridisch advies?
- [ ] Moet u het melden aan een regelgever of de politie?
- [ ] Moet u vanaf het begin een PR-medewerker inschakelen?

Denk dus na over wat er die dag zal gebeuren. U moet een plan hebben waarbij u geen losgeld betaalt.

Het is net als een brandoefening: u moet oefenen vóórdat het kantoor daadwerkelijk in brand staat. De actuele en meest waarschijnlijke aanvallen veranderen na verloop van tijd, dus u moet uw strategie en verdedigingstactieken regelmatig bijwerken. Download onze checklist voor ransomware om een begin te maken met uw plan.

Wees voorbereid op aanvallen

U moet bedenken wat er gaat gebeuren op het moment dat een aanval wordt geïdentificeerd en wanneer de aanval een datalek veroorzaakt. Kan de aanval worden beperkt tot een deel van uw infrastructuur door netwerkverkeer tegen te houden? Moet u systemen tijdelijk offline halen? Zo ja, wie neemt daarvoor de verantwoordelijkheid?

Snelheid is hierbij essentieel. Gerichte snelheid. U wilt niet hoeven wachten tot uw CTO terugbelt. Iedereen moet meteen weten wat te doen.

Als dit allemaal snel genoeg gebeurt, kunt u mogelijk zelfs de versleuteling voorkomen. U hebt ook een plan nodig om uw systemen snel te controleren zodat u precies weet wat er gaande is.

Moderne aanvallers gebruiken vaak meer dan één type aanval tegelijkertijd. Zo kunt u bezig zijn met een aanval waarbij de service wordt geblokkeerd, terwijl ergens anders een ransomwareaanval wordt uitgevoerd. Als u eenmaal weet wat er is gebeurd en waar, kunt u nadenken over wat u moet doen om de malware te vernietigen en de systemen weer online te krijgen.

Wanneer u de systemen en gegevens hebt hersteld, ofwel via een back-up of door de aanval tijdig te isoleren, en hebt gecontroleerd op corrupte of ontbrekende gegevens, is het tijd voor forensisch onderzoek.

Evalueer hoe effectief uw reactie was tegen een echte aanval. Analyseer wat goed werkte, wat alleen goed werkte vanwege geluk en waar nog verbeterpunten zitten. Denk na over hoe u uw reactie voor de volgende keer kunt verbeteren en versnellen.

Met de juiste beschikbare systemen beschikt u over een heleboel forensische gegevens. Mogelijk zelfs genoeg dat de politie een onderzoek kan starten. Welke gegevens u ook hebt, u moet even de tijd nemen voor een nabespreking met het reactieteam en nadenken over de geleerde lessen.

Nogmaals: dit gaat niet alleen over technologie, maar ook over mensen en processen. Moet u uw personeelstraining heroverwegen? Was uw reactieteam effectief of zit daar nog verbetering in?

Blijf op de hoogte

Tegenwoordig moeten verdedigingsstrategieën niet alleen reactief zijn, maar ook actief. U moet zoveel mogelijk transparantie in uw beveiligingssystemen hebben. U moet kunnen zien wat er gebeurt, wanneer en hoe vaak. Let op uw collega's: ransomwareaanvallers richten zich vaak op een specifieke verticale markt of geografie. Zorg er daarnaast voor dat u op de hoogte blijft van de nieuwste bedreigingen, trends en nieuws uit de branche met behulp van bronnen zoals de Barracuda-blog.

Gegevens zijn essentieel voor een goede beveiligingsstrategie. De positie of het profiel van uw organisatie verandert waarschijnlijk na verloop van tijd. U moet op de hoogte blijven en voorbereid zijn om deze verandering zo nodig door te voeren. Security-as-a-service kan helpen om makkelijker op de hoogte te blijven van ontwikkelingen, vooral nu het cyberbeveiligingslandschap van vandaag sneller dan ooit verandert.

Als een bedrijf een zeer actieve positie of een profiel met hoog risico heeft, kan dit betekenen dat er voltijd onderzoekspersoneel nodig is om vroeg te worden gewaarschuwd voor mogelijke aanvallen.

Voor de meeste organisaties is dit echter meer dan nodig is. Kies de juiste partner en zorg voor een goede basis. Echte aanvallers zijn, in tegenstelling tot in films en op tv, geen kwaadaardige genieën die de meest ingewikkelde beveiligingssystemen uitpluizen simpelweg omdat ze ervan houden. Over het algemeen zijn ze op zoek naar een makkelijke buit van iemand die steekjes heeft laten vallen en niet oplet of niet investeert in de juiste beveiliging.

Deze drie stappen (uw aanmeldgegevens beschermen, uw web applicaties beveiligen en een back-up maken van uw gegevens) bieden geen garantie dat u nooit door een ransomwareaanval wordt getroffen. U weet echter wel dat u nooit losgeld hoeft te betalen om uw gegevens terug te krijgen.

Over Barracuda

Bij Barracuda willen we de wereld een veiligere plek maken.

Wij geloven dat ieder bedrijf toegang verdient tot een cloud-enabled beveiligingsoplossing op bedrijfsniveau die makkelijk te kopen, implementeren en gebruiken is. Wij beschermen e-mails, netwerken, gegevens en toepassingen met innovatieve oplossingen die meegroeien en zich aanpassen aan het traject van onze klant.

Meer dan 200.000 organisaties over de hele wereld vertrouwen op Barracuda om hen veilig te houden, zelfs wanneer ze niet eens weten dat iets een risico vormt, zodat zij zich kun richten op hun bedrijf. Ga voor meer informatie naar barracuda.com.

Barracuda
Your journey, secured.