WHITE PAPER

RANSOMWARE IN PUCHASE-TO-PAY

ICREATIVE
PART OF 4CEE

Ransomware

Er zijn steeds meer cyberaanvallen in de vorm van Ransomware. Finance bevat op afdelingsniveau een schat aan gevoelige gegevens wat het aantrekkelijk maakt voor cybercriminelen om deze gegevens te gebruiken voor een zogenoemd gijzelvirus. En hoe meer menselijke handelingen daaraan te pas komen, des te kwetsbaarder de organisatie is voor cybercriminaliteit. Welk risico's lopen Basware gebruikers, welke voorzorgsmaatregelen zijn er en wat te doen bij een incident?

Facturen komen nog altijd vaak per e-mail binnen. Dit is een makkelijke ingang voor een virus, vooral als u werkt met een wat oudere applicatie. Omdat bijvoorbeeld Basware Invoice Processing (IP) werkt met een netwerklocatie (share) waar de factuurafbeeldingen en bijlagen worden opgeslagen – en gebruikers deze moeten kunnen toevoegen/ wijzigen/verwijderen – is dit een aandachtspunt.

Bij het gebruik van Basware Alusta (SaaS) is de afstand tot de bestandslocatie waar alles staat opgeslagen groter; er is geen directe koppeling anders dan de applicatielaag. Het voorportaal (Basware Network) is de enige manier om in de SaaSomgeving te komen.

Daarnaast betekent outsourcen van werkzaamheden ook het outsourcen van risicomanagement. Het risico is hier dus wat kleiner.

GEVOLGEN

Ransomware levert meer schade dan alleen losgeld. Ten eerste is er het uitzoekwerk na de constatering dat het netwerk geïnfecteerd is. Mogelijk is ook nog de privacy van klanten en/of leveranciers in gevaar gekomen. De IT-afdeling of helpdesk moet vervolgens het probleem isoleren en op zoek naar oplossingen.

Soms is er een decriptiesleutel voorhanden, maar in veel gevallen ook niet. Is die er niet, dan is de meest gangbare procedure dat het gedane werk wordt teruggehaald vanuit de meest recente back-up.

Veel bedrijven onderschatten echter wat een dag werk inhoudt: van het moment van de back-up tot het moment van de infectie. Wat er werkelijk is gedaan, welke data is gemuteerd en wat ervoor nodig is om het werk terug te krijgen.

De schade is vooral groot als er veel papieren facturen zijn gescand: vaak zijn die al weggewerkt of vernietigd.

Wat is Ransomware?

Om te weten welke voorzorgsmaatregelen Basware-gebruikers kunnen nemen, is het handig om even terug naar de basis te gaan en te begrijpen wat ransomware precies is en hoe het werkt.

Ransomware is een type malware welke systemen kan blokkeren en bestanden voorziet van een versleuteling waardoor deze niet langer meer bruikbaar zijn. Volgens de bijgeleverde ‘losgeld eis’ is de enige manier om het systeem en/of de bestanden te herstellen de betaling te doen.

In de meeste gevallen is de software afk omstig vanuit een zogenoemde ‘phishing’ mail met een link naar een malafi de website. Het kan ook zijn dat de mail een bijlage bevat (bijvoorbeeld een .docx of .xslx bestand met uitvoerbare code zoals een macro) die bij het openen het systeem zal infecteren.

Op het moment dat een systeem geïnfecteerd is zal het programma, afh ankelijk van het type, op zoek gaan naar bestanden met een specifi eke extensie (bijvoorbeeld .pdf;.tif;.asp).

Bij het zoeken naar deze bestanden zal niet alleen naar de lokale PC/laptop gekeken worden, maar ook naar netwerklocaties (shares) waar de gebruiker rechten toe heeft. Vervolgens zullen deze bestanden worden voorzien van een versleuteling op basis een zogeheten ‘asymmetrisch (RSA-2048 en AES128) codering algoritme’.

Doordat de bestanden voorzien zijn van een versleuteling zullen deze niet langer meer bruikbaar zijn. Naast een versleuteling zullen de bestanden ook hernoemd worden zodat ook niet meer te herleiden is welk versleuteld bestand bij welk origineel bestand hoort.

Dit heeft weer tot gevolg dat diverse applicaties die afh ankelijk zijn van deze bestanden, problemen kunnen vertonen.

In combinatie met Basware IP geeft het opstarten van de FAT-Client applicaties een foutmelding dat een bestand niet gevonden kan worden.

Welke voorzorgs-maatregelen zijn er?

Alle componenten in een extern netwerk is eigenlijk de enige volledige preventie. Het is niet mogelijk om een on-premise systeem volledig te beschermen tegen een infectie, maar diverse voorzorgsmaatregelen kunnen de gevolgen van een infectie wel minimaliseren. Zo is een CFO of finance manager verantwoordelijk voor bewustzijn bij zijn medewerkers en voor een impactanalyse. IT kan ook de nodige voorzorgs-maatregelen treffen.

De infectie begint altijd met een bron van buitenaf die door gebruikers onbewust op het systeem (binnen het netwerk) binnen wordt gehaald. Deze bron is veelal een phishing mail met een bijlage waarbij de afzender zich voordoet als een bestaand/bekend bedrijf om op die manier de ontvanger te overtuigen de bijlage te openen.

Het is dus van belang dat Basware-gebruikers de oorsprong van mails met dergelijke bijlagen goed controleren alvorens deze geopend worden.

De impact van een infectie is onder meer afhankelijk van de rechten die de (geïnfecteerde) gebruiker heeft op bestanden.

BASWARE NETWORK

Omdat e-mail het belangrijkste verspreidingsmechanisme van ransomware is, zou de eerste voorzorgsmaatregel zijn facturen niet langer te ontvangen via e-mail maar via een invoicing netwerk. Basware Network bijvoorbeeld biedt allerlei mogelijkheden voor ontvangst van facturen in inherent veilige bestandsformaten (xml, ubl 2.0, et cetera). Dat wil zeggen dat deze formaten in beginsel geen drager van een virus kunnen zijn. Daarnaast vinden er diverse controles plaats in Basware Network, die de beveiliging sterk verhogen. Ook wordt de afzender gecontroleerd, waardoor het vele malen lastiger wordt voor cybercriminelen om phishing facturen binnen het Basware Network te injecteren.
Last but not least, de verwerkingsketen van verzender tot ontvangst binnen Basware Alusta (SaaS of IP) of het ERP-systeem is volledig geautomatiseerd. Dus gebruikers kunnen niet worden ‘verleid’ tot phishing acties.

BASWARE ALUSTA

In Basware Alusta is de toegang tot de bestanden (factuurafbeeldingen e.d.) geregeld via een Service Account. Dit houdt in dat er een enkel account is met lees- en schrijfrechten tot deze share. Zolang de andere gebruikers geen rechten hebben om naar deze locatie te schrijven is de kans op encryptie door een infectie van ransomware dus minimaal. Een voorwaarde daarbij is dat het Service Account niet gebruikt dient te worden om in te loggen binnen Windows.

BASWARE IP

Voor Basware IP geldt dat gebruikers rechten nodig hebben op de zogenaamde BWRoot share waar de afbeeldingen, bijlagen, et cetera staan opgeslagen. Het kan zijn dat deze rechten niet altijd even goed zijn toegewezen waardoor mogelijk meer gebruikers toegang tot de netwerklocatie hebben dan strikt noodzakelijk – hierdoor is de kans dat de bestanden door niet Basware-gebruikers versleuteld worden onnodig groot.

Uit de praktijk is gebleken dat deze share geconfigureerd is zodat iedereen alle rechten heeft, mogelijk dat dit in de loop der tijd gewijzigd is om bepaalde problemen te verhelpen.

De matrix in figuur 1 geeft aan welke rechten gebruikers van respectievelijke applicaties minimaal nodig hebben om juist te kunnen werken.

Er kan gekozen worden om voor iedere applicatie een separate Active Directory (AD) groep in het leven te roepen en op die manier de rechten van gebruikers toe te wijzen.

Figuur 1 Minimale gebruikersrechten

Directory	ProClient	ThinClient	Monitor	Master	FastScan	Admin	Agent (service)
Root	R	-	R	R	R	R	-
Attach	RWM	RWM	R	RWM	-	-	-
Control	R	R	R	R	R	RWM	RWM
Help	R	R	R	R	R	R	-
Image	R	R	R	RWM	RWM	RWM	-
Lang	R	R	R	R	R	RW	-

R = Read
W = Write
M = Modify

ALGEMEEN

Verborgen share

Vanuit Microsoft Windows is het mogelijk om een netwerk share als “verborgen” te kenmerken; hierdoor zal deze niet naar voren komen bij het scannen van het netwerk door een apparaat. Indien de naam van de share bekend is en er voldoende rechten zijn, dan is de share wel vanaf ieder apparaat uit het netwerk te benaderen. Een verborgen share is te herkennen aan een “$” symbool achter de share naam. Door gebruik te maken van een dergelijke share is de kans op encryptie als gevolg van infectie door ransomware minimaal, aangezien deze de share niet zal vinden bij het scannen van het netwerk. Enkel wanneer er bijvoorbeeld een netwerkschijf gekoppeld is naar deze share zal dit een aandachtspunt zijn.

Back-up

Het maken van een back-up geeft de mogelijkheid om de data te herstellen naar een eerder moment in de tijd. Het interval waarmee of de manier waarop de back-up is gemaakt is van invloed op de hoeveelheid data die verloren gaat bij een herstelactie.

Als bijvoorbeeld dagelijks om 00:00 een back-up wordt gemaakt en om 14:00 worden bestanden versleuteld door Ransomware, dan zal bij het herstellen van de bestanden alle nieuwe of gemuteerde data in de periode van de back-up en het moment van infectie verloren gaan.

Het advies is daarom om met een hoge regelmaat een back-up te maken van deze gevoelige informatie (in het bijzonder de informatie in de mappen “Attach” en “Image” die zich in de BWRoot share bevinden) om zo het risico van dataverlies te minimaliseren.

Antivirus

Een belangrijk onderdeel van preventie is om eventuele infecties in de kiem te smoren door het gebruik van up-to-date antivirussoftware op de pc’s/laptops van gebruikers.

Indien wenselijk kan ICreative een ondersteunende rol spelen bij de analyse van de huidige rechtenconfiguratie op de Basware (BWRoot) share. Daarbij kan ICreative een advies geven van welke acties in gang kunnen worden gezet om de beveiliging – indien van toepassing – te verbeteren.

Deze werkzaamheden vallen buiten regulier support en worden om die reden op basis van Time & Materials gefactureerd.

Wat te doen bij infectie?

Ieder probleem kent ook zijn eigen oplossingen, zo ook ransomware. In de loop van de jaren is deze vorm van Malware geëvolueerd naar een vaak niet te kraken algoritme, echter is er vanuit diverse instanties een tegenoffensief geïnitieerd.

Op de website www.NoMoreRansom.org (een initiatief van Europol, European Cybercrime Centre, National High Tech Crime Unit van de Nederlandse politie, Kaspersky Lab en Intel Security) staat aanvullende informatie over de historie van ransomware, advies over preventie en andere zaken zoals decryptie hulpmiddelen.

Het NoMoreRansom-project heeft een tool om te achterhalen of er een decryptie-mogelijkheid is voor de betreff ende infectie. Dit kan getest worden met de zogenaamde “Crypto Sheriff ” door een tweetal geïnfecteerde bestanden te uploaden en informatie uit de losgeldbrief (vaak

een html pagina in de map met geïnfecteerde bestanden). Indien een decryptie mogelijkheid bestaat zal deze beschikbaar worden gesteld.

BETALING

Is er geen decryptiemogelijkheid is de meest voor de hand liggende oplossing om de gijzelnemers te betalen. Het is sterk af te raden om dit te doen omdat er geen garantie is dat de bestanden ook daadwerkelijk na betaling worden vrijgegeven. Daarnaast houdt dit het concept ransomware alleen maar in stand.

BACK-UP TERUGZETTEN

Zoals al eerder bij het hoofdstuk over preventie aangegeven, is het mogelijk om via een back-up de bestanden in Basware te herstellen. Hierbij is het van belang om te kiezen hoeveel informatie de organisatie bereid is te verliezen. Als er bijvoorbeeld dagelijks een back-up van de data wordt gemaakt, is het verlies bij het teruggaan naar een back-up maximaal 24 uur aan data. In het geval van Basware IP dienen gebruikers er rekening mee te houden dat bij het terugzetten van een back-up er een verschil zal ontstaan tussen de informatie in de database (die namelijk niet geraakt is door de infectie en het terugzetten van de backup) en de informatie op het bestandssysteem. Overleg daarom altijd met ICreative of alle nodige – relevante – informatie is veiliggesteld alvorens men de back-up terugzet

Interessant?

Wil je meer weten over onze oplossingen?
Kijk op icreativep2p.com voor meer informatie.

Nieuwsgierig naar de mogelijkheden die wij te bieden hebben? Nodig ons uit voor een vrijblijvend gesprek.

Over ICREATIVE

ICreative levert purchase-to-pay en e-facturatie oplossingen aan ambitieuze ondernemingen, instellingen en overheden. Onze oplossingen vergroten de controle op bedrijfsuitgaven en verkleinen de complexiteit van inkoop en factuurverwerking.

Vraag een adviesgesprek aan