CASE STUDY

Cyberaanval in de praktijk

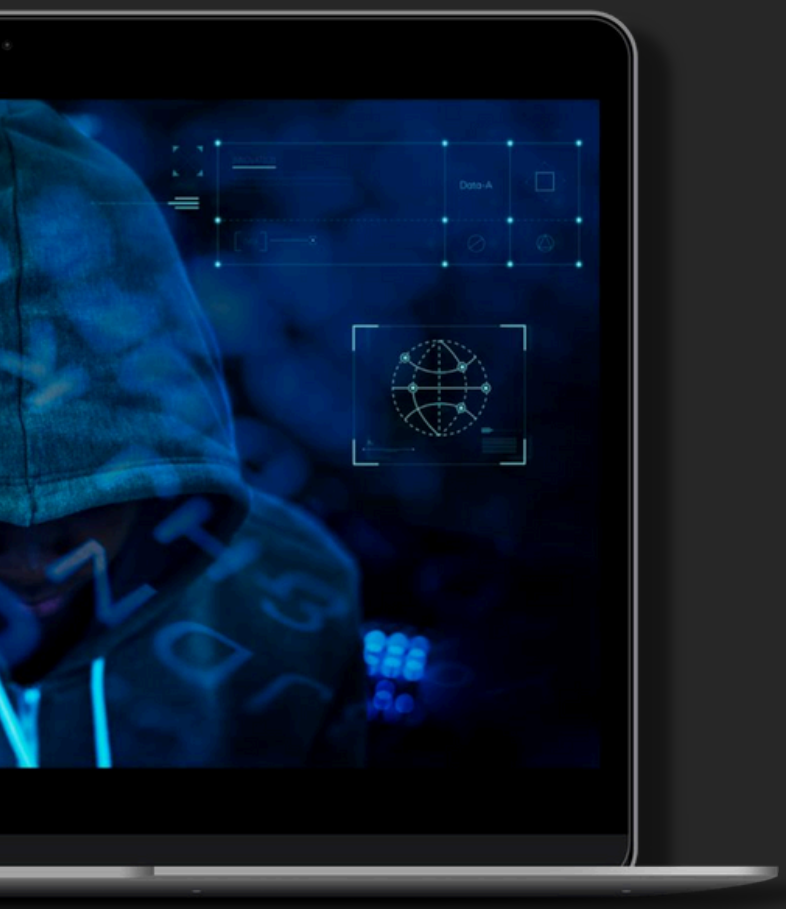
INCL. TIPS & TRICKS OM EEN RANSOMWARE AANVAL OP UW BEDRIJF TE VOORKOMEN

KAAP HOORN ICT SECURITY B.V. 2024

INHOUD

INLEIDING

In 2023 meldde 45% van de bedrijven wereldwijd slachtoffer te zijn geweest van een ransomware-aanval. Omdat ransomware zich steeds verder ontwikkelt, kan zelfs de eenvoudigste vorm ervan veel tijd en geld kosten.



WAT IS RANSOMWARE?

Ransomware is een type kwaadaardige software (malware) dat dreigt gegevens of een computersysteem openbaar te maken of de toegang ertoe te blokkeren. Dit gebeurt meestal door ze te versleutelen totdat het slachtoffer losgeld betaalt aan de aanvaller. In veel gevallen gaat de losgeldeis gepaard met een deadline. Als het slachtoffer niet op tijd betaalt, zijn de gegevens voor altijd verdwenen of wordt het losgeld hoger.

Ransomware-aanvallen komen tegenwoordig maar al te vaak voor. Enterprise ransomware-infecties beginnen meestal met een kwaadaardige e-mail. Een nietsvermoedende gebruiker opent een bijlage of klikt op een kwaadaardige of gecompromitteerde URL. MKB-bedrijven over de hele wereld zijn er al slachtoffer van geworden. Cybercriminelen vallen elke consument of elk bedrijf aan, en de slachtoffers komen uit alle sectoren. U dient dus snel noodzakelijke maatregelen te treffen om uw netwerken te beveiligen tegen hackers.

HOE WERKT RANSOMWARE?

Ransomware is een type malware dat is ontworpen om geld af te persen van slachtoffers door hun toegang tot gegevens of systemen te blokkeren. De twee meest voorkomende typen ransomware zijn encryptors en screen lockers. Encryptors, zoals de naam al aangeeft, versleutelen gegevens op een systeem, waardoor de inhoud onbruikbaar wordt zonder de decryptiesleutel.

Screen lockers daarentegen blokkeren eenvoudigweg de toegang tot het systeem met een vergrendelscherm, waarbij wordt beweerd dat het systeem is versleuteld. Slachtoffers worden vaak op een vergrendelscherm gewaarschuwd (zowel bij encryptors als screen lockers) om een cryptocurrency, zoals Bitcoin, te kopen om het losgeld te betalen. Zodra het losgeld is betaald, ontvangen slachtoffers de ontsleutelingssleutel en kunnen ze proberen bestanden te ontsleutelen. Ontsleuteling is echter niet gegarandeerd, aangezien meerdere bronnen melden dat er wisselend succes is met het ontsleutelen na het betalen van losgeld. Soms ontvangen slachtoffers de sleutels nooit.

DE CASE

TIP: "Maak alvast een firewallregel aan die al het uitgaande verkeer blokkeert en test deze regel zodat je hem bij een aanval direct kunt activeren. Controleer daarnaast welke poorten worden gebruikt door bedrijfskritische applicaties en maak hier uitzonderingen voor. Dit voorkomt lange downtime en zorgt ervoor dat het IT-personeel zich kan richten op de aanval."

Vincent Mosk | Pentester bij Kaap Hoorn ICT Security

30 maart 2022 - 18:53

De telefoon gaat, het is onze partner die ons voorziet van pentest opdrachten. Een klant is gehackt en is ten einde raad of er iemand beschikbaar is om te helpen. Ik vraag intern om hulp en neem ondertussen contact op met de klant om de situatie te bespreken. In recordtijd is er een crisisteam ingericht om de situatie te bespreken. Ransomware stopt of vermindert de productiviteit van een bedrijf, dus de eerste stap is beheersing.

Uit initieel onderzoek blijkt dat er een datastroom naar Roemenië is, dus als eerste stap hebben we het online verkeer naar Roemenië afgesloten en de desbetreffende server geïsoleerd. Bij het starten van een volledige antimalwarescan werden er sporen gevonden van Cobalt Strike, een veelgebruikt stuk software om netwerken aan te vallen met als doel het ontdekken van kwetsbaarheden.

Omdat de aanvaller nu waarschijnlijk weet dat hij/zij is gedecteerd en daarom kan overgaan tot bijvoorbeeld het anctiveren van ransomware hebben we de stap genomen om al het uitgaande verkeer te blokkeren om te voorkomen dat de malware kon communiceren met de servers van de aanvallers. Dit creëerde tijd om uit te zoeken wat er precies gebeurde op het netwerk.

MONITOREN

TIP: "Zorg dat er reeds een systeem aanwezig is dat de eventlogs van alle apparatuur verzamelt en deze kan correleren. Wanneer de software achteraf wordt geïnstalleerd, gaat er kostbare tijd en geld verloren die op het moment van een aanval beter ingezet kan worden. Tevens heb je hierdoor niet direct alle data van de aanval van voor de installatie tot je beschikking."

Vincent Mosk | Pentester bij Kaap Hoorn ICT Security

Nadat het verder isoleren van het netwerk onder controle is, is het belangrijk om inzicht te creëren. Wie of wat is er aanwezig op het platform en hoe kun je zo snel mogelijk verdachte activiteit signaleren en waar is patient zero?

Aangezien er geen ogen en oren in het netwerk was hebben we ervoor gekozen om op alle servers SentinelOne (Endpoint Detection and Response) en Rapid7 IDR (Security Information and Event Management) te installeren, zodat er als het ware een vangnet over het netwerk wordt uitgegooid om verdachte activiteiten te monitoren en vervolgens daarop te kunnen acteren. Binnen Rapid7 zijn diverse bronnen toegevoegd, zogenaamde Event Sources, zodat logs worden verzameld van allerlei activiteiten op basis waarvan abnormaal gedrag wordt gesignaleerd.

We hebben ook een honey user uitgerold, een account dat niet aan een echt persoon gekoppeld is maar aantrekkelijk is om mee in te loggen, op de servers en werkstations. Zodra de hacker het wachtwoord van dit account achterhaalt en probeert in te loggen op een andere server, genereert dit een melding en kan het betreffende apparaat worden geïsoleerd.

Omdat Rapid7 IDR nog niet was uitgerold toen de aanval plaatsvond, hebben we samen met een forensisch bedrijf sporen onderzocht om de servers en werkstations te controleren waarop verdachte activiteiten waren waargenomen. Dit om zeker te weten dat de aanvaller ook echt uit het netwerk was.

Nadat we dit zeker wisten, zijn we een voor een begonnen met het herstellen van systemen. Hierbij lag de focus op het zo snel mogelijk herstellen van de productie en ervoor zorgen dat medewerkers weer aan het werk konden. Ook is er tijdens het herstel veel aandacht besteed aan het hardenen van systemen en het verhelpen van kwetsbaarheden.

TIP 1

Bepaal welke systemen zijn aangetast. U moet systemen isoleren zodat ze de rest van de omgeving niet kunnen beïnvloeden. Deze stap maakt deel uit van het inperken van de schade aan de omgeving.

TIP 2

Koppel systemen los en schakel ze zo nodig uit. Ransomware verspreidt zich snel via het netwerk. Raadpleeg cybersecurity-experts voordat u drastische maatregelen neemt, omdat het abrupt uitschakelen van een machine dataverlies of verlies van belangrijk forensisch bewijs kan veroorzaken.

TIP 3

Stel prioriteiten bij het herstel van systemen zodat de meest kritieke systemen sneller kunnen worden hersteld. Ons advies is om de prioriteit te baseren op de productiviteit, de impact op de inkomsten en de continuïteit.

TIP 4

Verwijder de bedreiging uit het netwerk. Aanvallers kunnen backdoors gebruiken, dus de uitroeiing moet worden uitgevoerd door een vertrouwde deskundige. De expert moet toegang hebben tot logboeken zodat hij/zij een analyse van de hoofdoorzaak, de kwetsbaarheid en alle getroffen systemen kan identificeren.

TIP 5

Laat een professional de omgeving controleren op mogelijke beveiligingsupgrades via een audit of pentest. Het komt vaak voor dat een slachtoffer van ransomware een doelwit is voor een tweede aanval. Als de kwetsbaarheid niet wordt gevonden, kan deze opnieuw worden uitgebuit.

CONCLUSIE

TIP: "Reset alle wachtwoorden van accounts met hoge privileges. Log niet direct in met admin-accounts op servers, want de wachtwoorden worden lokaal gecached en kunnen door de aanvallers worden uitgelezen. Log in met gepersonaliseerde accounts en verhoog de rechten alleen bij specifieke acties met een admin-account."

Kasper de Waard | Pentester bij Kaap Hoorn ICT Security

CONCLUSIE

Omdat de aanval snel werd waargenomen, kon het netwerk snel geïsoleerd worden en bleef een verdere ransomware-aanval uit. Het uitzoeken hoe de aanval is ontstaan, het deblokkeren van alle uitgaande traffic en het herstellen van de systemen heeft meerdere weken geduurd. Uiteindelijk zijn er drie cybersecuritypartijen bij betrokken geweest.

Het is belangrijk om regelmatig beveiligingsonderzoeken uit te voeren en de juiste procedures en tools van tevoren op orde te hebben, zodat er snel kan worden gereageerd op een eventuele aanval. Dit scheelt kostbare downtime op het netwerk, met alle financiële gevolgen van dien.

U kunt zelf ook een paar basisstappen nemen om goed te reageren op ransomware, zoals het bijhouden van up-to-date back-ups en het trainen van personeel in cybersecuritybewustzijn. Toch is de tussenkomst van een expert meestal vereist voor de analyse van de hoofdoorzaak, opschoning en onderzoek. Het kan ook nuttig zijn om te kijken naar proactieve beveiligingsmaatregelen, zoals threat hunting en continue monitoring, om uw netwerk beter te beschermen tegen toekomstige aanvallen.

Voorkomen is beter dan genezen.

Bent u na het lezen van deze case study benieuwd hoe wij uw bedrijf kunnen helpen bij het beveiligen van uw informatiestructuren en de bescherming tegen hackers? Neem dan geheel vrijblijvend contact op 0229 799 800. Of e-mail kasperdewaard@kaaphoorn.net