C-SOC

Ransomware

De nieuwe dreiging van het digitale tijdperk

Introductie

Ransomware is ondertussen uitgegroeid tot een van de meest beruchte vormen van cybercriminaliteit. Maar wat is Ransomware precies?

We hebben het over kwaadaardige software die gemaakt is om belangrijke, gevoelige data op een computer of netwerk te versleutelen. Deze versleuteling kan vervolgens door de hacker ongedaan worden gemaakt wanneer de gedupeerde bereid is om een hoog bedrag aan losgeld of bitcoins te betalen. Er is momenteel een explosie aan aanvallen wereldwijd, en deze treffen niet meer enkel de grote corporates maar ook overheidsinstellingen en zelfs individuen.

In dit e-book willen we in een beknopt verhaal inzicht bieden in hoe Ransomware werkt en hoe we ons hier tegen kunnen beschermen.

Inhoud

Hoe Ransomware in zijn werk gaat

Ransomware verspreidt zichzelf op verschillende manieren, zoals phsihing e-mails, dubieuze downloads, kwetsbaarheden in software of zelfs via het dark web. Zodra Ransomware een systeem is binnengedrongen, begint het met het versleutelen van data waardoor de eigenaar machteloos staat.

Vaak is Ransomware al binnen enkele minuten na het binnendringen effectief, afhankelijk van de omvang van het systeem en de complexiteit van de software die wordt gebruikt door de hacker.

Zodra het versleutelen is gelukt, krijgt de gedupeerde een bericht waarin staat uitgelegd hoe het losgeld of de bitcoins betaald moeten worden waarna de decryptiesleutel zal worden toegestuurd.

Ransomware is niet enkel een technisch probleem maar kan de economie en samenleving op grote schaal benadelen. Daarom vinden we het belangrijk om de ernst hiervan met u te delen zodat we begrijpen hoe deze dreiging zich evolueert.

De psychologie achter Ransomware

Als we weten wat de motivatie is achter een Ransomware aanval, zullen we beter begrijpen hoe groot de omvang van deze dreiging is. Er zijn verschillende redenen voor een hacker om Ransomware in te zetten. Zo stelt het ze in staat om op een relatief simpele manier snel aan veel geld te komen met een kleine pakkans. Door in te spelen op angst en onzekerheid bij hun slachtoffer, geven hackers mensen het gevoel dat het betalen van het geëiste bedrag de enige manier is om hun data te redden. Dit is niets minder dan psychologische manipulatie wat een krachtig wapen is waarmee geprofiteerd wordt van een wanhopige gedupeerde.

Helaas is het probleem met het betalen van losgeld vaak nog niet opgelost. Een bedrijf kan na een Ransomware aanval te maken krijgen met verlies van productiviteit, reputatieschade, juridische kosten of zelfs boetes van regelgevende instanties als gevolg van een inbreuk op gegevensbeveiliging. Naast dit alles brengt het herstel van een getroffen systeem vaak ook veel tijd en hoge kosten met zich mee, waardoor de impact soms blijvend is.

Populaire Ransomware groepen

Ranswomware aanvallen worden meestal uitgevoerd door georganiseerde hack-groepen die erom bekendstaan op een geavanceerde en meedogenloze manier te werk te gaan. Hieronder noemen we een aantal van deze groepen waar u wellicht al eens van hebt gehoord, of in de toekomst nog van zult horen.

Ryuk: deze groep wordt vaak geassocieerd met impactvolle aanvallen op bedrijven en organisaties over de hele wereld. Ze gebruiken verwoestende Ransomware varianten en richten zich hiermee op grote bedrijven, overheidsinstellingen of gezondheidsorganisaties.

Maze: door het gebruik van innovatieve methoden zet deze groep slachtoffers onder druk om hoge bedragen te betalen. Ze dreigen met het openbaar maken van gestolen data waardoor gedupeerde bedrijven onder druk worden gezet om snel te zwichten. Maze heeft een meedogenloze reputatie en gebruikt geavanceerde Ransomware, wereldwijd.

REvil/Sodinokibi: in het huidige cyberlandschap staat deze groep erom bekend grote organisaties aan te vallen en enorme losgeldbedragen te eisen.

Populaire Ransomware groepen

Ze richten zich vaak op bedrijven met aanzienlijke financiële middelen en gevoelige data, zoals juridische instanties, financiële instellingen en tech-bedrijven.

Locky: als een van de eerste grote Ransomware groepen, verspreidt Locky schadelijke software via phishing mails of dubieuze downloads. Hun populariteit is niet zo zeer tegenomen maar ze blijven een prominente rol spelen binnen de cybercriminaliteit. Hun aanvallen zijn vaak gericht op kleine bedrijven of individuele gebruikers.

Bovenstaande groepen geven slechts een kleine weergave van de vele Ransomware verspreiders wereldwijd. Het is belangrijk dat we ons bewust zijn van de reële dreiging, zowel privé als zakelijk!

Data diefstal en chantage

In de afgelopen jaren is het gebruik van Ransomware enorm gegroeid door de opkomst van data diefstal en dubbele chantage technieken. Deze ontwikkeling heeft ervoor gezorgd dat de impact van zo'n aanval tegenwoordig zeer groot is en veel uitdagingen met zich meebrengt voor de slachtoffers.

Data diefstal

Een traditionele Ransomware aanval is ingericht om bestanden te versleutelen waardoor de eigenaar geen toegang meer heeft, totdat hij of zij toegeeft door losgeld te betalen. Echter onlangs zijn er nieuwe tactieken opgedoken waarbij deze bestanden, vaak gevoelige informatie, eerst gestolen wordt. Hierdoor kan er veel druk worden uitgeoefend op de gedupeerde doordat er gedreigd wordt met het openbaar maken van deze data, met reputatieschade en schending van privacy als gevolg.

Dubbele chantage

Hiermee wordt bedoeld dat een hacker niet alleen losgeld eist van het slachtoffer, maar óók dreigt om de gestolen, privacygevoelige informatie openbaar te maken.

Data diefstal en chantage

Deze dubbele dreiging geeft de aanvaller de mogelijkheid om een nóg hogere druk uit te oefenen en maakt de inzet voor het slachtoffer veel hoger. Bedrijven en organisaties moeten nu niet alleen de financiële consequenties overwegen maar ook de eventuele gevolgen van reputatieschade en juridische problemen.

Deze ontwikkelingen benadrukken het belang van proactieve beveiligingsmaatregelen en effectieve responsmethoden. C-SOC kan u helpen bij het beschermen van uw kostbare data!

Bescherming tegen Ransomware

Wat kunt u doen om u en uw gegevens te beschermen tegen potentiële Ransomware aanvallen? Hieronder geven we een aantal tips.

- **Antivirus- en anti-malwaresoftware**: het is belangrijk dat alle devices uitgerust zijn met up-to-date antivirus en anti-malware programma's. Hiermee wordt schadelijke software snel gedetecteerd en kan er direct actie worden ondernomen om schade te beperken.
- **Patch management:** werk software, systemen en applicaties bij met de nieuwste beveiligingspatches om bekende kwetsbaarheden te verhelpen.
- **E-mailbeveiliging:** installeer spamfilters en authenticatieprotocollen om phishing mails en schadelijke bijlages direct te detecteren.
- **Endpointbeveiliging:** gebruik beveiligingsoplossingen zoals firewalls, IDS/IPS en EDR om verdachte activiteiten direct te kunnen detecteren en te voorkomen dat Ransomware de kans krijgt zich te verspreiden binnen het netwerk.
- **Back-ups:** maak regelmatig back-ups van belangrijke gegevens en sla deze op op een aparte, offline locatie om te voorkomen dat ze in de verkeerde handen vallen.

Bescherming tegen Ransomware

Dit zijn slechts enkele stappen die genomen moeten worden om uzelf en uw data te beschermen tegen cybercriminaliteit. Hier is veel tijd en specialistische kennis voor nodig, waarvan wij ons kunnen voorstellen dat u deze liever aan uw core business besteedt!

Met behulp van Microsoft Defender zorgen onze cybersecurity analisten ervoor dat uw IT-omgeving 24 uur per dag, 7 dagen per week optimaal beschermd is tegen dreigingen van buitenaf. Onze diensten zijn onderverdeeld in drie pakketten:

ZILVER MDR

24/7 detection & response

- ✓ Endpoint monitoring
- ✓ E-mail monitoring
- ✓ Basis identiteitsmonitoring
- ✓ Cloud App monitoring
- ✓ Maatwerk detectieregels
- ✓ Maandelijkse incidentenrapport

GOUD MXDR

24/7 detection & response

Als aanvulling op alle voordelen van pakket Zilver, krijgt u bij Goud ook:

- ✓ Vulnerability management advies
- ✓ Awareness academy
- ✓ Threat hunting
- ✓ Doorlopende rapportage

MEEST GEKOZEN

PLATINUM MXDR

24/7 detection & response

Als aanvulling op alle voordelen van de pakketten Zilver en Goud, krijgt u bij Platinum ook:

- ✓ Netwerk logbronnen
- ✓ 3rd Party logs
- ✓ Data loss prevention
- ✓ Aanvullende identiteitsmonitoring
- ✓ Threat hunting+

Benieuwd welk pakket het beste past bij uw organisatie? We gaan graag in gesprek om samen te bespreken wat uw beveiligingsbehoeftes zijn!

Bent u nieuwsgierig geworden naar wat C-SOC voor u kan betekenen?

We komen graag in contact om u in een vrijblijvend gesprek de vele mogelijkheden en voordelen uit te leggen voor u als MSP.

C-SOC

www.c-soc.nl | verkoop@c-soc.nl