4 Best Practices voor ransomware-gereedheid

Insight

Een korte geschiedenis van ransomware

Vanaf de begindagen van de locker-gebaseerde Trojaanse aanvallen die vanaf 1989 plaatsvonden, is ransomware van een kleine zorg uitgegroeid tot een van de belangrijkste bedreigingen op het gebied van cyberbeveiliging. Toen encryptie begin jaren 2000 onderdeel werd van de aanvalsstrategie, begon ransomware echt een bedreiging te worden en ontwikkelde zich nog sneller tussen 2010 en 2020.

Deze groeispurt vond deels plaats door de opkomst van Bitcoin als een handige methode voor het betalen van losgeld die de anonimiteit van de kwaadwillende partijen beschermde, en deels door het succes van exfiltratie-achtige aanvallen (ook wel leakware of doxware), waarbij kwaadwillende partijen dreigden gevoelige data openbaar te maken, als er geen losgeld zou worden betaald.

Ransomware over een periode van 40 jaar

1989

De eerste bekende ransomware-aanval, een trojan horse, wordt gelanceerd.[1]

1999

Toename van thuis-pc's en e-mailvirussen brengen cyberbeveiliging onder de aandacht van het algemene publiek.[2]

2009

Bitcoin komt op de markt, waardoor afpersing eenvoudiger wordt voor kwaadwillende partijen.[3]

2019

Exfiltratie en afpersing beginnen de ransomwarestrategie te domineren.[4]

2029

Het banenaanbod in de cyberbeveiliging behoort tot het snelst groeiende, met een verwachte stijging van 31%.[5]

Ransomware-trends van vandaag

Ransomware-aanvallen zijn in kracht en ernst gegroeid en de bijbehorende kosten zijn gestegen naarmate het aantal getroffen organisaties groeit en back-ups falen als een effectieve verdedigingsstrategie.[6,7]

De gemiddelde losgeldbetaling stijgt:

KW1 - 2021:	**KW2** - 2021:	**KW3** - 2021:	**KW4** - 2021:
$111.605	**$178.254**	**$139.739**	**$322.168**[8]

$265 MILJARD Totale ransomwarekosten voor alle bedrijven in 2030[9]

70% van organisaties kreeg in 2021 te maken met een ransomware-aanval. **Meer dan 63% van deze organisaties betaalde het losgeld.**[10]

Ransomware heeft elke **2 seconden** impact op **1 bedrijf.**[11]

Gemiddelde uitvaltijd per aanval **15 dagen**[12]

Topdoelen voor ransomware per sector:

1: **Technologie** 2: **Gezondheidszorg** 3: **Onderwijs**[13]

Het gemiddelde IT-beveiligingsbudget voor 2022 is **$ 24,4 miljoen**, waarvan **25%** naar verwachting zal worden besteed aan ransomwaremitigatie[14].

Ransomware is een toenemende bedreiging die proactieve strategie en een meerlaagse aanpak vereist. Het onderkennen van de kansen op en financiële gevolgen van een aanval is slechts het begin.

Wat zijn uw volgende stappen?

In deze handleiding leert u de vier primaire componenten van effectieve gereedheid voor en reactie op ransomware kennen.

1. Ken uw kwetsbaarheden

Ransomware gebruikt de kwetsbaarheden van een organisatie om de omgeving te infiltreren. Er zijn twee fundamentele aspecten waar u rekening mee moet houden bij het beoordelen van de kwetsbaarheden van uw organisatie:

A. Elke laag van uw IT-omgeving levert risico's op.

Ransomwarebescherming begint met een full-stack overzicht van uw hele infrastructuur. Aanvallers hebben maar één zwakke plek nodig om binnen te komen. Het identificeren en aanpakken van bestaande beveiligingsproblemen op elk niveau van uw organisatie, van netwerkbeveiliging tot back-uparchitecturen en meer, moet de hoogste prioriteit hebben.

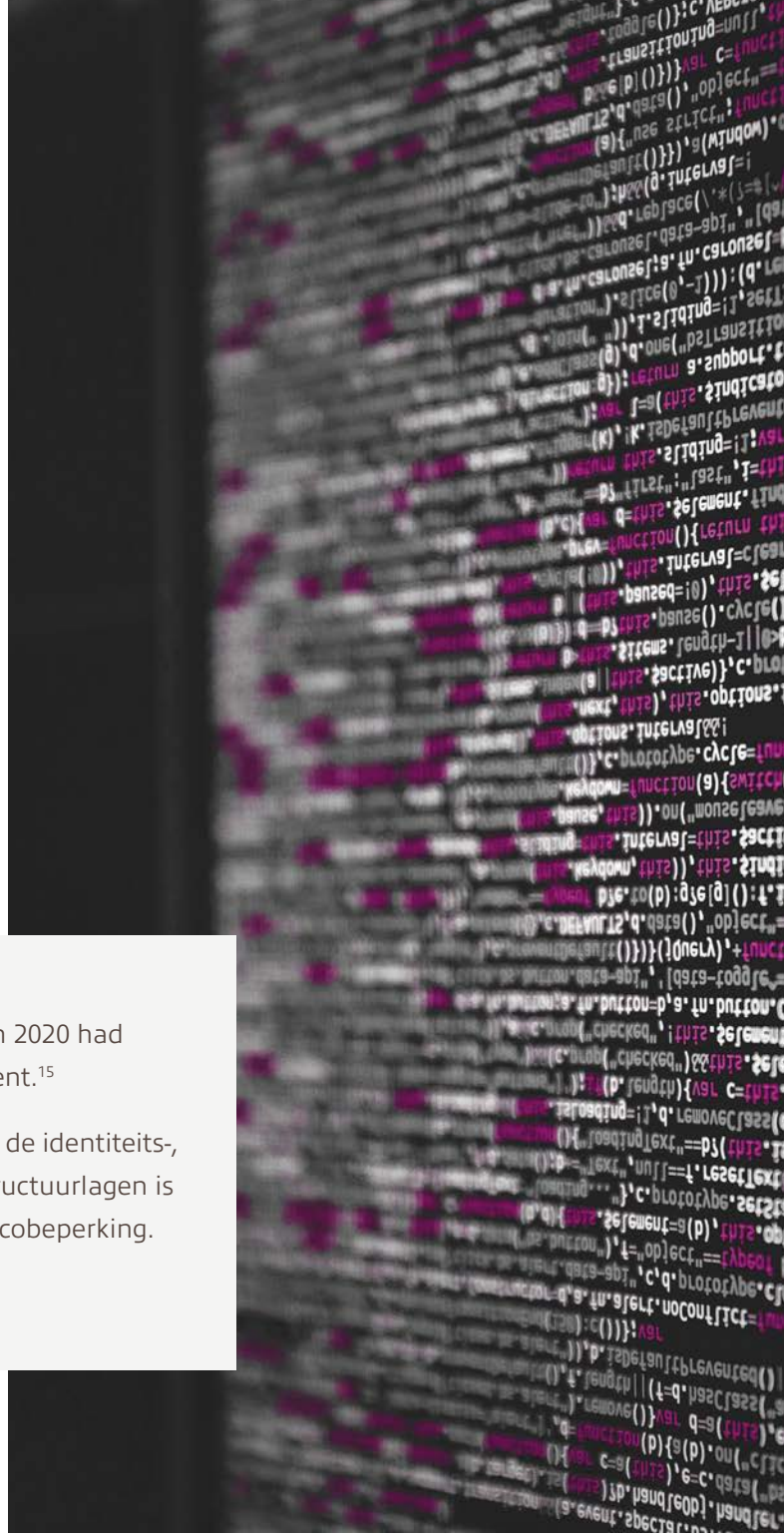
B. Menselijke fouten zijn de oorzaak van de meest succesvolle ransomware-aanvallen.

De prevalentie van menselijke fouten is zo diepgaand dat de meeste ransomware-aanvallen erop vertrouwen. Hoewel ransomware is geëvolueerd, vertrouwen de meeste aanvallen nog steeds op een eindgebruiker die per ongeluk inloggegevens verstrekt of klikt voor het activeren van een kwaadaardig programma.

Hoewel het misschien nooit mogelijk zal zijn om het probleem van menselijke fouten volledig op te lossen, is het mogelijk om uw risico's te minimaliseren en de gaps op te vullen met goed gebouwde architecturen en goed geïmplementeerde beveiligingsprotocollen in uw volledige organisatie.

85% van de inbreuken in 2020 had een menselijk element.[15]

Het creëren van beveiliging op de identiteits-, endpoint-, netwerk- en infrastructuurlagen is cruciaal voor uitgebreide risicobeperking.



2. Uw data beveiligen

De dingen die u gaat overwegen voor het beveiligen van uw data beginnen bij begrijpen wat u probeert te beschermen. De prevalentie van exfiltratieaanvallen kan worden gekoppeld aan de toenemende waarde van data en de groeiende hoeveelheden gevoelige data die wordt gegenereerd, opgeslagen en gebruikt door organisaties met een hoog risico.

Onveranderlijkheid van data is een ander punt om te overwegen. Dat wil zeggen, het creëren van data die niet kan worden gewijzigd nadat het is geschreven. De term komt vaak naar voren in gesprekken over ransomware. In theorie is het een praktische oplossing. In de praktijk kan het moeilijk zijn om dit te bereiken. Vooral wanneer uw aanvallers gebruikmaken van toegang tot interne controles om uw back-upomgevingen in gevaar te brengen, maar we gaan het hier verder over hebben in het volgende gedeelte.

Vanwege de moeilijkheid van daadwerkelijke onveranderlijkheid van data is het van cruciaal belang om ervoor te zorgen dat uw databeschermingsplatform veilig is. Hoewel deze overweging nog steeds belangrijk is voor data on premise, moeten organisaties extra voorzichtig zijn bij het beschermen van data opgeslagen in de cloud.

Er wordt algemeen aangenomen dat data automatisch veiliger is in de cloud. Dit is echter volledig bezijden de waarheid. Cloudserviceovereenkomsten adviseren vaak specifiek om een externe bron voor databescherming te gebruiken. Vergeet niet: U bent verantwoordelijk voor uw data.

Volg een datagerichte aanpak en stel de vraag:

"Met welke soort data heb ik te maken?"

"Waar bevindt deze data zich?"

"Hoe beschermen we dit?"

Als u al deze vragen kunt beantwoorden, hebt u een veel sterkere basis om mee te beginnen.

3. Maak een back-up van uw back-ups

Databack-ups werden lange tijd beschouwd als het primaire plan in geval van een aanval. Nu? Back-ups zijn waar de aanvallers beginnen. Het werkt ongeveer zo:

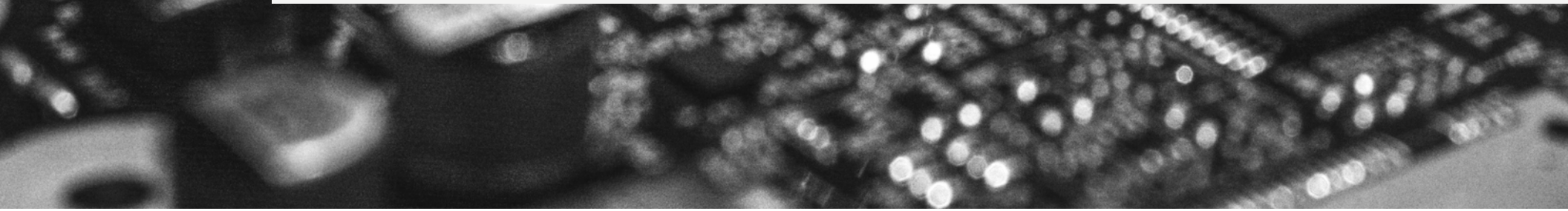
Uw back-upsoftware en -architectuur zijn geweldig; u denkt dat u beschermd bent. Dan maakt iemand in uw organisatie een uitglijder. Hierdoor krijg een aanvaller de admin-aanmeldgegevens in handen. Met deze aanmeldgegevens kunnen ze tijd doorbrengen in uw omgeving, uw back-upproces leren kennen en vervolgens de back-ups aanvallen voordat ze hun ransomware loslaten. Nu is uw failsafe verdwenen en is de kans groter dat u het losgeld betaalt om toegang te krijgen tot uw resterende data.

> "Ik heb klanten gehad die alle juiste stappen hadden gezet met betrekking tot het hebben van back-upapparaten, het repliceren van data tussen twee datacenters, enz. Maar het waren niet de back-upsoftware of de apparaten zelf die een probleem vormden. Het was ofwel een standaardwachtwoord of iemand die de admin-aanmeldgegevens in gevaar heeft kunnen brengen. **Ze kwamen binnen en wisten in principe de back-upapparaten en lieten vervolgens de ransomware los.**"
>
> — **Data Protection Solutions Architect**, Insight

Alleen back-ups zijn niet genoeg en back-ups in de cloud betekenen niet dat uw data veilig zijn. Back-ups waren veiliger toen netwerken en fysieke perimeters gemakkelijker te beveiligen waren. Maar met de evolutie van thuiswerken en Internet of Things (IoT) zijn perimeters moeilijker te definiëren en te beveiligen, waardoor het nog belangrijker is om uw back-upomgevingen te controleren en passende strategieën voor dataisolatie/air gap te hebben.

De beste manier om uw data te beschermen tegen ransomware is door:

- Meerdere kopieën van de data te hebben
- Meerdere mediatypen te gebruiken
- Het op te slaan op meerdere locaties, bij voorkeur ook off-site



4. Te zorgen voor een plan (en test, wijzig en oefen het)

Er zijn veel dingen die u kunt doen om uw risico op ransomware-aanvallen te verminderen, maar er is geen enkele manier om ze volledig te voorkomen. De beste aanpak is om u voor te bereiden alsof u zeker weet dat u een datalek zult ervaren omdat de kans statistisch gezien groot is.

> "U moet er niet van uitgaan of het gaat gebeuren, maar wanneer. Dus, zijn we er op voorbereid en wat gaan we doen?"
>
> — **Lead Architect**, Insight

Planning

Het ontwikkelen van een disaster recovery-plan is een cruciaal en vaak over het hoofd gezien onderdeel van de ransomwarepuzzel. Van netwerkbeveiligingsoverwegingen tot juridische implicaties: evalueer alle mogelijke gevolgen van een ransomware-gebeurtenis en stel een actieplan samen. U kunt samenwerken met beveiligingsserviceprofessionals om een aangepast, uitvoerbaar incidentresponsplan te creëren. Te veel organisaties hebben beperkte herstelplannen die alleen ergens in iemands hoofd opgeslagen zijn. Het is ook belangrijk dat het plan goed is gedocumenteerd en voor uw hele organisatie geldt.

Testen

Net zo belangrijk als het ontwikkelen van een plan is het testen ervan. Test uw plan in uw huidige omgeving op eventuele gebreken, pas het indien nodig aan en oefen het tijdig, en blijf het herzien indien nodig. Dit zorgt er niet alleen voor dat interne teams klaar zijn om snel en effectief te reageren in het geval van een gebeurtenis, maar dat uw plan ook actueel en optimaal gepositioneerd is voor de beste resultaten.

Onderwijs

Volgens data van IBM is slechts 38% van de werknemers van overheden getraind in de preventie van ransomware, wat vooral zorgwekkend is gezien de hoeveelheid risico waarmee publieke organisaties worden geconfronteerd.[16]

Met menselijke fouten als belangrijkste reactie op de ransomwareketen, kan voorlichting niet over het hoofd worden gezien.

Alle personen binnen een organisatie moeten een basistraining krijgen over ransomware, met name hoe ze phishing- en spoofing-aanvallen kunnen herkennen en melden.

Ransomware is er klaar voor. Bent u dat ook?

De aanpak voor ransomware van elke organisatie zal uniek zijn. Een effectieve strategie houdt rekening met verschillende factoren, waaronder de hoeveelheid en aard van uw data en de complexiteit van uw IT-infrastructuren.

Insight kan u helpen bij het evalueren van uw huidige beveiligingspositie met betrekking tot de zich ontwikkelende dreiging van ransomware, door samen met u te werken aan een holistische benadering voor cyberbeveiliging die elke laag van uw IT-omgeving beschermt en voldoet aan de specifieke behoeftes van uw organisatie.

Als u klaar bent voor een gesprek over de manieren waarop u de gereedheid ten opzichte van ransomware van uw organisatie kan verbeteren, neem dan contact met ons op.

nl.insight.com

Bron:
[1] Kassner, M. (2010, 11 jan). Ransomware: Extortion via the Internet. TechRepublic.
[2] FBI. (2019, 25 maart). The Melissa Virus: An $80 Million Cyber Crime in 1999 Foreshadowed Modern Threats. FBI.gov.
[3] Bernard, Z. (2018, 10 nov.). Everything you need to know about Bitcoin, its mysterious origins, and the many alleged identities of its creator. Business Insider.
[4] Siegel, B. (2020, 10 jan.). The Marriage of Data Exfiltration and Ransomware. Security Boulevard.
[5] Columbus, L. (2020, 1 nov.). What Are The Fastest Growing Cybersecurity Skills in 2021? Forbes.
[6] FBI. (2019, 2 oktober). High-Impact Ransomware Attacks Threaten U.S. Businesses And Organisations. PSA: https://www.ic3.gov/Media/Y2019/PSA191002.
[7] Robinson, T. (2020, 7 dec.). Ransomware attacks target backup systems, compromising the company 'insurance policy.' SCmagazine.com.
[8] Coveware Quarterly Ransomware Report. (2021, 3 feb.). Law enforcement pressure forces ransomware groups to refine tactics in Q4 2021.
[9] Braue, D. (2021, 3 juni). Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031. Cybersecurity Ventures.
[10] CyberEdge Group. 2022 Cyberthreat Defense Report.
[11] Braue, D. (2021, 3 juni). Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031. Cybersecurity Ventures.
[12] Kass, D.H. (2022, 13 jan.). Supply Chain Security and Ransomware Attacks: CrowdStrike Research Findings. MSSPAlert.
[13] Gruber, D. en Lundell, B. (feb. 2020). Ransomware Still Rampant, Fueled by Insurance Companies. Enterprise Strategy Group.
[14] Gately, E. (2022, 24 feb.). The High Cost of Ransomware. ChannelFutures.
[15] Burbidge, T. (2021, 13 mei). Cybercrime thrives during pandemic: Verizon 2021 Data Breach Investigations Report. Verizon.
[16] The Harris Poll. (2020). Public Sector Security Research: IBM-Harris Poll Survey 2020. On behalf of IBM Security.

MKT6203_NL