De Amitron Zero Risk Anti-ransomwarelijst

De 10 maatregelen om jouw organisatie tegen ransomware-aanvallen te beschermen

Wat zijn de risico's waar we mee te maken hebben?

Een relatief onbeduidend stukje software kan tot grote kopzorgen leiden. In december 2021 werd een kwetsbaarheid in de veelgebruikte, maar voor velen onbekende Java-library Apache Log4j gevonden. Via deze kwetsbaarheid kunnen hackers op afstand de controle overnemen over computers en andere devices waarop bepaalde versies van Log4j draaien. Volgens het Amerikaanse CISA (Cybersecurity and Infrastructure Security Agency) gaat het om honderden miljoenen kwetsbare devices: van computers in cloudsystemen tot aan smart-homeproducten.

Serieuze schadelijke kwetsbaarheden zoals die in Apache Log4j maken vrijwel alle organisaties acuut kwetsbaar. Naar verwachting worden velen van hen de komende tijd helaas het slachtoffer van cyberaanvallen, met name ransomware-aanvallen waarbij computerdata wordt 'gegijzeld'. Dit type aanvallen is de afgelopen jaren explosief gestegen. De FBI heeft in de eerste helft van 2021 maar liefst 62% meer meldingen van ransomware-incidenten ontvangen dan in dezelfde periode in 2020!

Hoe voorkom je dat jouw organisatie een van de volgende slachtoffers is? Amitron heeft een lijst van tien maatregelen tegen ransomware-aanvallen opgesteld: ***de Amitron Zero Risk Anti-ransomwarelijst***. Met die maatregelen maak je je organisatie immuun tegen geslaagde aanvallen en/of de schade ervan. In deze whitepaper vertellen we je meer over ransomware en zetten we de maatregelen uit de Amitron Zero Risk Anti-ransomwarelijst op een rijtje.

Wat is ransomware?

Ransomware is malware (kwaadaardige software) die de data van het slachtoffer (een organisatie of persoon) opzettelijk versleutelt, zodat die er niet meer bij kan. Pas als het slachtoffer 'losgeld' betaalt aan de hacker die achter de ransomware-aanval zit, geeft die - hopelijk - de data weer vrij. In het Nederlands wordt ransomware ook wel 'gijzelsoftware' genoemd.

Als bij een ransomware-aanval daarnaast persoonsgegevens geraakt zijn, is er formeel sprake van een datalek. Afhankelijk van het type organisatie dat is getroffen, moet dit slachtoffer het datalek rapporteren aan de Autoriteit Persoonsgegevens. Die kan eventueel een boete opleggen. Een extra reden om bedacht te zijn op ransomware-aanvallen!

Hoe wordt een ransomware-aanval uitgevoerd?

De drie meest voorkomende routes die ransomwarehackers volgen om je organisatie binnen te komen, zijn:

1) Phishing e-mails
2) Zwakke wachtwoorden
3) Systeemkwetsbaarheden

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

Phishing e-mails

Een phishing-e-mail bevat een schadelijke bijlage of een link naar een malafide website. De aanvaller verstuurt de e-mail naar zijn slachtoffer. Als die de bijlage of de link opent, wordt de ransomware op zijn computer geïnstalleerd.

Zwakke wachtwoorden

Zwakke wachtwoorden zoals ‘geheim01’ of ‘1234’ zijn makkelijk te achterhalen. Hetzelfde geldt voor standaardwachtwoorden die een softwareleverancier heeft ingesteld en die nooit door de gebruiker zijn veranderd. Als een aanvaller het zwakke wachtwoord van een systeemaccount weet te kraken, kan hij eenvoudig toegang krijgen tot het systeem. Vervolgens installeert hij de ransomware.

Systeemkwetsbaarheden

Wie niet regelmatig software-updates installeert, loopt gevaar. Oude versies van software bevatten vaak kwetsbaarheden die ook bij aanvallers bekend zijn. Een aanvaller kan zo’n kwetsbaarheid uitbuiten om via de achterdeur toegang tot een systeem te krijgen en de ransomware te installeren.

Neem de 10 Amitron Zero Risk-maatregelen om je organisatie immuun te maken tegen aanvallen en de schade door ransomware.

De 10 Zero Risk-maatregelen tegen ransomware

Een goede bescherming tegen ransomware is een combinatie van:

1) maatregelen die de installatie van ransomware voorkomen
2) maatregelen die een ransomware-aanval tijdig detecteren en verwijderen
3) maatregelen die de door ransomware veroorzaakte schade herstellen

Neem de volgende tien noodzakelijke maatregelen om je organisatie een sluitende bescherming tegen ransomware te bieden:

1. E-mail- en domeinauthenticatie

In hun phishing-e-mails geven aanvallers zich vaak uit voor iemand anders, iemand die door het slachtoffer wordt vertrouwd. Daarbij gaan de aanvallers zover dat ze zelfs - als het even kan - voor de verzending een e-mailadres gebruiken met daarin de domeinnaam van de vertrouwde partij. Zo lijken hun mails nog authentieker.

Gebruik **e-mail- en domeinauthenticatie** om jezelf en anderen tegen dit misbruik van e-maildomeinen te beschermen. Je laat dan op je mailsysteem strenge authenticatiecontroles uitvoeren op inkomende en uitgaande e-mailberichten: is een bericht inderdaad afkomstig van een bekend mailsysteem van de veronderstelde afzender? Zo niet, dan weigert het ontvangende mailsysteem de e-mail voordat die in een mailbox wordt afgeleverd.

Om e-mail- en domeinauthenticatie in te stellen, moet je de configuratie van je domein en je mailsystemen aanpassen. De e-mailbeveiligingsprotocollen SPF, DKIM en DMARC beschrijven welke instellingen hiervoor moeten worden gebruikt.

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

2. E-mail sandboxing

Stel: je ontvangt een e-mail waarin een bestand via een link of als bijlage is meegestuurd. Hoe weet je of het veilig is om dat bestand te openen? Je kunt er natuurlijk achterkomen door het gewoon te proberen. Maar dan loop je het risico dat het bestand een onderdeel van een ransomwareaanval is en schade toebrengt aan je computersysteem.

Er bestaat antimalware-software die e-mailbijlagen en -links kan vergelijken met een lijst van bekende malware. Dat helpt al iets, maar wat als de bijlage of link een nog onbekende vorm van malware is? Gebruik sandboxing om ook deze uiterst gevaarlijke nieuwe bedreigingen te detecteren.

Een sandboxing-product analyseert de links en bijlagen van een e-mail om vast te stellen of het openen van de bestanden schadelijke gevolgen kan hebben. Dat gebeurt in een veilige, geïsoleerde omgeving binnen je computer of (in het geval van een cloud- of netwerkoplossing) daarbuiten: de sandbox. Op die manier heeft de analyse geen effect op de (rest van) je computersysteem, ook niet als het bestand malware blijkt te bevatten.

Bijlagen die malware bevatten of links die naar malware verwijzen worden door de sandboxing-technologie tegengehouden, zodat je ze niet kunt downloaden, openen en activeren.

3. Sterke wachtwoorden met multifactorauthenticatie

Voorkom het gebruik van zwakke wachtwoorden binnen je organisatie. Stel daartoe een **wachtwoordbeleid** op voor je medewerkers. Daarin leg je onder andere vast aan welke eisen een wachtwoord moet voldoen: hoeveel karakters moet het wachtwoord minimaal bevatten? Welke speciale karakters moeten daartussen zitten? Hoe vaak moet een wachtwoord worden ververst? Dwing deze eisen waar mogelijk technisch af.

Verplicht daarnaast **multifactorauthenticatie (MFA)**: het gebruik van een tweede authenticatiemiddel naast de combinatie van gebruikersnaam en wachtwoord. Dat werpt een extra drempel op voor aanvallers die toegang tot een account proberen te krijgen. Voorbeelden van zo'n tweede authenticatiemiddel zijn fysieke en mobiele tokens die een tijdelijke inlogcode genereren.

Pas de combinatie van sterke wachtwoorden en MFA toe op *elke* externe toegang tot je data en netwerk: via remote access, VPN, RDP, Citrix, Office 365 enzovoorts.

4. Segmentatie van netwerk, data en back-up

Deel je bedrijfsnetwerk op in logisch gescheiden segmenten (subnetten). Zorg dat niet alles voor iedereen beschikbaar is: plaats belangrijke data in een subnet dat met aanvullende toegangsmaatregelen is beschermd. Zo voorkom je dat een aanvaller zich snel en ongehinderd door het netwerk kan verplaatsen, op zoek naar de kostbaarste data.

5. User-awarenesscampagnes

Vergissen is menselijk. Bij IT-beveiliging zijn menselijke gebruikers dan ook de zwakste schakels. Maar met de juiste training kunnen gebruikers daarentegen een goede verdedigingslinie vormen tegen cyberaanvallen, als een soort menselijke firewall.

Maak **user-awareness** een permanent onderdeel van het trainingsprogramma voor je medewerkers. Geplande, korte, periodieke videotrainingen die constant in een bepaalde vorm blijven terugkeren, houden je huidige en nieuwe werknemers blijvend op de hoogte van bedreigingen, zoals ransomware. Besteed in de training ook aandacht aan de verwachte handelingen na het opmerken van een bedreiging.

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

6. Vulnerability-management, patching en vulnerability-protection

Zorg dat je IT-systemen up-to-date zijn. Daarmee voorkom je dat een ransomware-aanvaller kwetsbaarheden in verouderde software kan misbruiken. Een **vulnerability-managementsysteem of -service** helpt je om deze kwetsbaarheden te identificeren.

Richt daarnaast een efficiënt **patchproces** in om de nodige patches (beveiligingsupdates) te installeren en gevonden kwetsbaarheden te dichten.

Niet elke kwetsbaarheid is direct op te lossen met een patch, bijvoorbeeld omdat een patch simpelweg nog niet beschikbaar is of - in het geval van oudere systemen - zelfs niet meer beschikbaar komt. Of omdat het installeren van een patch tot compatibiliteitsproblemen leidt. Pas daarom ook actieve vulnerability-protectiontechnologie op systemen of netwerken toe die tijdelijke of permanente kwetsbaarheden in systemen immuun maakt tegen specifieke, gerichte aanvallen.

7. Cryptokiller

Ongewenste versleutelingsprocessen zijn een duidelijk symptoom van een ransomware-aanval in uitvoering. Een **cryptokiller-technologie** kan deze processen op een systeem detecteren en stoppen. Vervolgens kunnen beschadigde bestanden worden hersteld. Pas deze technologie toe op de endpoints en servers van je organisatie.

8. Endpoint-detectie en -response

Verschillende signalen kunnen duiden op een (beginnende) cyberaanval tegen je organisatie, waaronder:

1) verdachte bestanden op devices van je organisatie
2) verdachte processen op devices van je organisatie, bijvoorbeeld het zoeken naar en wijzigen van bepaalde informatie in het register van Windows
3) verdacht dataverkeer op het bedrijfsnetwerk van je organisatie
4) verdachte verbindingen tussen devices in je bedrijfsnetwerk en de buitenwereld

Zet **endpoint-detectie- en responsetechnologie** in om je bedrijfsnetwerk en devices te monitoren op zulke signalen. Dat geeft inzicht in wanneer een aanval begint en hoe die zich door de organisatie ontwikkelt. Zo kun je effectief reageren voordat het te laat is en werken aan herstel naar de originele situatie.

Dit inzicht in aanvalspogingen is ook noodzakelijk om een eventuele datalekmelding naar de Autoriteit Persoonsgegevens van de juiste verplichte informatie over de aanval en tegenmaatregelen te voorzien - en zo boetes te helpen voorkomen.

9. Back-up

Back-ups zijn een must voor het herstellen van verloren data. Dat is niet anders voor data die bij een ransomware-aanval zijn versleuteld. Zorg daarom voor een effectief **back-upplan en bijbehorende technologie** voor alle omgevingen van je organisatie: on-premise en in de cloud (zoals Microsoft 365).

Segmenteer de data in een apart netwerk, zodat je niet één grote back-up krijgt op één plaats, maar bijvoorbeeld verschillende back-ups per omgeving en applicatie. Vervolgens pas je de 3-2-1-methode toe voor het maken van de back-ups:

1) Maak minimaal 3 kopieën van de data

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

2) Zet de kopieën op 2 verschillende media
3) Sla 1 van de media op op een andere locatie

Zorg daarnaast voor het volgende:

1) Voer periodieke controles uit op de werking van de back-up en restore
2) Versleutel de back-up
3) Zorg dat back-ups nooit verwijderd kunnen worden, ook niet door de administrators zelf

10. Cybersecurityverzekeringen

De schade van een ransomware-aanval kan aanzienlijk zijn. Volgens de State of Ransomware 2021 betaalden organisaties die het slachtoffers waren van ransomware-aanvallen in 2021 gemiddeld $170.404 aan losgeld voor hun data. Slechts 8% van die organisaties kreeg alle data terug na betaling. Hierbij is berekend dat de totale kosten voor het herstel van een ransomware-aanval ongeveer tien keer zoveel zijn als het betaalde losgeld - gemiddeld meer dan 1 miljoen dollar! Die kosten zitten onder andere in misgelopen inkomsten door downtime.

Sluit daarom een **cybersecurityverzekering** af om je organisatie te dekken tegen de schade en herstelkosten van een ransomware-aanval. Een goede verzekering helpt je ook om het proces van herstel en het inroepen van een afhandelingsspecialist te versnellen. Heel belangrijk, want bij een ransomware-aanval telt elke seconde.

Aan de slag met de Amitron Zero Risk Anti-ransomwarelijst

In deze whitepaper hebben we 10 technische en organisatorische maatregelen beschreven die je moet nemen om je organisatie immuun te maken voor ransomware-aanvallen: de Amitron Zero Risk Anti-ransomwarelijst.

Wil je hiermee aan de slag, maar mis je de nodige expertise in jouw organisatie? Wij helpen je graag verder met toegespitst advies.

Neem contact op met Amitron: info@amitron.nl, telefoon: 010 - 870 01 50.

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl