Negen aanbevelingen

Ransomware en de rol van een IT-Auditor

11 november 2021

Kunter Orpak

(Publicatiedatum: 11 november 2021)

Ransomwareaanvallen zijn met een snelle opmars bezig en staan internationaal inmiddels op de tweede plaats in de ranglijst van cyberbedreigingen. IT-auditors kunnen veel betekenen voor organisaties om ransomware-risico's te mitigeren. Dit artikel geeft hiervoor een aantal handvatten en doet negen concrete aanbevelingen.

Ransomware is een type malware die bestanden en systemen versleutelt om losgeld te eisen voor het weer toegankelijk maken ervan. [CSBN2021] Ransomware verstoort en stopt de processen van een organisatie en stelt het management voor een dilemma: moet de organisatie losgeld betalen of proberen haar data en IT-systemen met behulp van backups zelf te herstellen? In 2021 zijn ransomware-aanvallen de tweede bron van cyberaanvallen. [THAL2021] Deze aanvallen bieden cybercriminelen een aantrekkelijk verdienmodel, wat blijkt uit het gegeven dat 82 procent van de slachtoffers in de eerste helft van 2021 het geëiste losgeld hebben betaald. [PALO2021]

Ransomware kill chain

Een ransomware-aanval staat niet op zichzelf. [CSBN2021] Het is een onderdeel van een breder proces, de *kill chain*, waarbij verschillende stappen kunnen worden onderscheiden, zie figuur 1.

Figuur 1: De ransomware kill chain [CSBN2021]

Continu misbruikte kwetsbaarheden

In de afgelopen jaren werden kwetsbaarheden in mondiaal gebruikte producten continu misbruikt om initiële toegang te verkrijgen tot de systemen en ransomware in te zetten. Kwetsbaarheden in Pulse Secure Connect VPN, Fortinet FortioOS Secure Socket Layer VPN, Atlassian Confluence Server en Microsoft SharePoint zijn enkele voorbeelden van veelgebruikte producten die misbruikt zijn. [CISA2021a]

Continu misbruikte kwetsbaarheden	CVE[1] en Score CVSS[2]	Ransomware Campagne
Pulse Secure Connect VPN	CVE 2019-11510 - Kritiek	Sodinokibi en Netwalker
Fortinet FortioOS Secure Socket Layer VPN	CVE 2018- 13379 - Kritiek	Cring
Atlassian Confluence Server	CVE 2019- 3396 - Kritiek	GandCrab
Telerik UI for ASP.NET AJAS Insecure Deserialization	CVE 2019- 18935 - Kritiek	Netwalker
Microsoft SharePoint	CVE 2019- 0605 - Kritiek	WickrMe en Hello
Windows background Intelligent Transfer Service Elevation of Privilege	CVE 2020- 0787 - Hoog	Maze en Egregor

Figuur 2: Continu misbruikte kwetsbaarheden [CISA2021a]

Het gebruiken van end-of-life software in de IT-infrastructuur en default-wachtwoorden zijn momenteel de prominente *bad practices* die buitengewone cyberrisico's vormen voor de organisaties. [CISA2021c]

Ransomware-as-a-Service (RaaS)

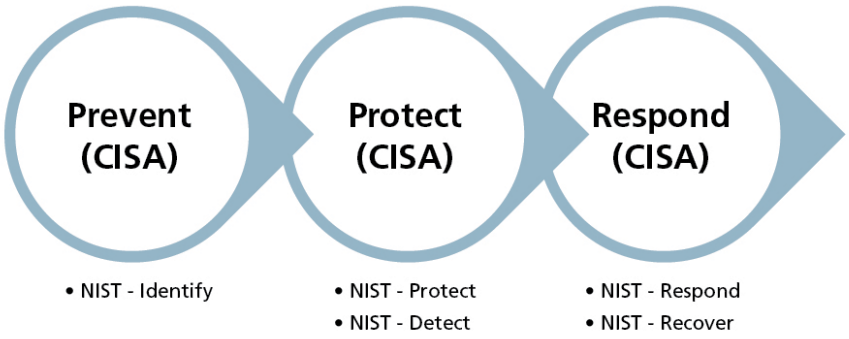
Ransomware-as-a-service (RaaS) is een dienstenmodel voor *pay-for-use malware*. Dienstverleners van RaaS bieden ransomware-malware aan als hun product en dienst. Ransomware-ontwikkelaars hebben dit model ontwikkeld om hun malware op grote schaal te verspreiden zonder zelf risico te lopen. Via RaaS kunnen criminelen op eenvoudige wijze over ransomware beschikken, waarbij ze een vast overeengekomen percentage van het betaalde losgeld aan de ransomware-ontwikkelaars betalen. [SECU2021] Enkele voorbeelden van RaaS zijn Lockbit, Maze, REvil en Ryuk. [TECH2021]

Cybercriminelen zijn altijd op zoek naar nieuwe zwakke plekken om ransomware-aanvallen uit te voeren. Lockbit 2.0 is daar een goed voorbeeld van. De LockBit-

ransomware is al een tijdje actief en wordt aangeboden als een RaaS, maar vanaf de tweede helft van dit jaar werven de ontwikkelaars van Lockbit 2.0 medewerkers van de potentiële slachtoffers om hen te helpen in netwerken binnen te dringen en bestanden te versleutelen. Miljoenen dollars zijn beloofd aan deze insiders in ruil voor hun samenwerking. [BLEE2021]

Specifieke publicaties over ransomware

Organisaties kunnen zowel preventieve, detecterende als corrigerende maatregelen implementeren om hun IT-systemen te beschermen tegen ransomware-aanvallen. Er zijn een aantal nieuwe initiatieven opgestart door overheidsinstellingen in de VS om ondernemingen te helpen mitigerende maatregelen tegen de ransomware-aanvallen te implementeren. Enkele goede voorbeelden zijn de recente publicaties van de Cybersecurity & Infrastructure Security Agency (CISA) en het National Institute of Standards and Technology (NIST).[3] Het concept NIST-cybersecurity framework is specifiek opgesteld voor ransomware riskmanagement. [NIST2021] De publicatie van CISA richt zich specifiek op het beschermen van gevoelige en persoonlijke data tegen ransomware-aanvallen. [CISA2021b] Zie figuur 3 voor de overeenkomsten tussen deze twee stappenplannen.



Figuur 3: Stappen om ransomware-risico te beheersen. [NIST2021] en [CISA2021b]

Rol van een IT-auditor

IT-auditors kunnen deze nieuwe raamwerken in hun assurance- en adviesopdrachten gebruiken als referentiekaders. Ze kunnen hiermee de belangrijkste ransomware-risico's en ontbrekende maatregelen onder de aandacht van directie en raad van commissarissen brengen. Hieronder zijn enkele voorbeelden voor IT-auditors uit deze raamwerken samengevat:

Prevent

1. *Offline backup & recovery:* Na een ransomware-aanval kan een organisatie met behulp van backups haar data en IT-systemen herstellen, maar de belangrijkste vuistregel is dat de organisatie over offline backups beschikt. IT-auditors kunnen controleren of de organisatie over offline en versleutelde backups beschikt en de organisatie periodiek test of de back-up, en het terugzetten hiervan, correct werkt.
2. *Cyber incident response plan:* IT-auditors kunnen controleren of het cyber incident response plan van een organisatie, waarin escalatieprocedures voor ransomware-incidenten beschreven zijn, toereikend is. Daardoor kunnen de herstelwerkzaamheden snel uitgevoerd worden en kan schade als gevolg van een ransomware-incident beperkt worden.
3. *Internet-facing kwetsbaarheden:* IT-auditors kunnen controleren of organisaties tools gebruiken om kwetsbaarheden geautomatiseerd te inventariseren en deze kwetsbaarheden risicogestuurd op te volgen. Cybercriminelen krijgen vaak initiële toegang tot een netwerk via slecht beveiligde remote services. [CISA2021b] IT-auditors kunnen netwerksystemen auditen die Remote Desktop Protocol (RDP) gebruiken. Ze kunnen beoordelen dat ongebruikte RDP-poorten gesloten zijn en multi-factor authenticatie (MFA) gebruikt wordt. Ze kunnen ook vaststellen dat de organisatie actief met behulp van tools de datastroom vanuit het bedrijfsnetwerk naar buiten monitort.
4. *Phishing:* voor het verhogen van het beveiligingsbewustzijn van de medewerkers is een security awareness-programma cruciaal. IT-auditors kunnen nagaan in welke mate onder meer presentaties, phishing-campagnes, mystery guests en e-learnings onderdeel uitmaken van het security awareness-programma.
5. *Insider threat:* het monitoren van personeelsactiviteiten kan organisaties helpen insider threats tijdig te detecteren. IT-auditors kunnen controleren of organisaties over een mitigatieprogramma voor insiders threats beschikken. Verder kunnen ze nog soft controls meenemen bij de beoordeling van hun bevindingen. Per bevinding kunnen ze een oorzaakanalyse uitvoeren waarin de gedrags- en cultuuraspecten betrokken zijn. [IIA2015]

Protect

1. *Kroonjuwelen:* IT-auditors kunnen controleren of kroonjuwelen zoals primaire processen, servers en databases waarin gevoelige/persoonlijke data is opgeslagen, in kaart zijn gebracht.
2. *Netwerksegmentatie en firewalls:* IT-auditors kunnen controleren of de organisaties netwerksegmentatie, *firewalls en Intrusion Detection System/ Intrusion Prevention System* (IDS/IPS) hebben toegepast om de toegang tot de IT-systemen te beperken tot geautoriseerde personen en IT-services.
3. *Encryptie:* het toepassen van actuele encryptietechnieken op netwerkverbindingen zijn belangrijk om exfiltratie van data te beperken [NIST2021]. IT-auditors kunnen

controleren of gevoelige en persoonlijke *data-at-rest en data-in-transit* met toereikende technieken zijn versleuteld.

Respond

1. Consulting-rol: in het reageren op een ransomware-incident spelen de IT-auditors nauwelijks een rol. De IT-afdeling, security office en security-dienstverleners zijn direct betrokken bij de fasen analyse, containment, eradication en recovery. [CISA2020d] In het kader van de consulting-rol van de IT-auditors kunnen ze samenwerken met deze functies, zodat deze functies noodzakelijke acties ondernemen om de hieruit volgende schade zoveel mogelijk te beperken. IT-auditors dienen bij deze werkzaamheden aandacht te besteden aan de wijze waarop organisatie omgaat met een ransomware-incident en de afwikkeling hiervan. Ze kunnen nagaan of de juiste functies en partijen zijn betrokken in de besluitvorming van deze fase.

Tot slot

Er is een toename van het aantal ransomware-aanvallen vanaf begin 2021. In 2021 staan ze op de tweede plaats van het totaal aantal type cyberaanvallen. Ransomwareaanvallen bieden cybercriminelen een aantrekkelijk verdienmodel en ze zijn daarom op zoek naar nieuwe zwakke plekken om ransomware-aanvallen uit te kunnen voeren. Zoals in dit artikel is aangegeven, kunnen IT-auditors veel betekenen voor organisaties om ransomware-risico's te mitigeren. Zie ook het tekstkader 'Negen aanbevelingen voor IT-auditors'.

Negen aanbevelingen voor IT-auditors

1. **Offline en versleutelde backups**. Controleer of de organisatie over offline en versleutelde backups beschikt en de organisatie periodiek test of de back-up en het terugzetten hiervan adequaat werkt.
2. **Cyber incident response plan**. Beoordeel of het cyber incident response plan van de organisatie de escalatieprocedures voor ransomware-incidenten toereikend adresseert.
3. **Toolgebruik**. Controleer of de organisatie tools gebruikt om kwetsbaarheden geautomatiseerd te inventariseren en risicogestuurd op te volgen.
4. **Security awareness**. Beoordeel de toereikendheid van security awareness-programma van de organisatie.
5. **Insider threats**. Controleer of de organisatie over een mitigatieprogramma voor insider threats beschikt.
6. **Kroonjuwelen**. Beoordeel of kroonjuwelen van de organisatie inzichtelijk zijn gemaakt.
7. **Technische maatregelen**. Controleer of de organisatie netwerksegmentatie, firewalls en IDS/IPS heeft toegepast.
8. **Encryptie**. Controleer of de gebruikte encryptietechnieken op netwerkverbindingen actueel zijn.
9. **Organisatorische procedures**. Beoordeel de wijze waarop de organisatie omgaat met een ransomware-incident en de afwikkeling hiervan.

Noten

[1] CVE, *Common Vulnerabilities and Exposures*, is een databank met informatie over kwetsbaarheden in computersystemen en netwerken. De Databank wordt onderhouden door de organisatie MITRE Corporation.

[2] CVSS, *Common Vulnerability Scoring System* is een gratis en open standaard om de ernst van securitykwetsbaarheden van computersystemen te beoordelen.

[3] Cybersecurity and Infrastructure Security Agency (CISA): https://www.cisa.gov/, NIST Computer Security Resource Center: https://csrc.nist.gov/.

Literatuur

[BLEE2021], *LockBit ransomware recruiting insiders tobreach corporate networks*, 2021, https://www.bleepingcomputer.com/news/security/lockbit-ransomware-recruiting-insiders-to-breach-corporate-networks/, geraadpleegd op 4 augustus 2021.

[CISA2020d], *Ransomware Guide*, 2020, https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf, geraadpleegd op 1 september 2020.

[CISA2021a], *Top Routinely Exploited Vulnerabilities* https://us-cert.cisa.gov/ncas/alerts/aa21-209a, geraadpleegd op 28 juli 2021.

[CISA2021b], *Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches*, 2021, https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf, geraadpleegd op 18 augustus 2021.

[CISA2021c], *Bad Practices*, 2021, https://www.cisa.gov/stopransomware/bad-practices, geraadpleegd op 2021.

[CSBN2021], *Cybersecuritybeeld Nederland*, 2021, https://www.nctv.nl/binaries/nctv/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021/CSBN2021_def_interactieve+pdf_web.pdf, geraadpleegd op 28 juni 2021.

[IIA2015], *Soft controls*, 2015, https://www.iia.nl/SiteFiles/Publicaties/IIA_Bro_A4_Soft_Controls_03.pdf, geraadpleegd op 1 juni 2015.

[NIST2021], *Cybersecurity Framework Profile for Ransomware Risk Management*, 2021, https://csrc.nist.gov/CSRC/media/Publications/nistir/draft/documents/NIST.IR.8374-preliminary-draft.pdf, geraadpleegd op 1 juni 2021.

[PALO2021], *Unit 42 Ransomware Threat Report*, 2021, https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/, geraadpleegd op 9 augustus 2021.

[SECU2021], *Australische overheid waarschuwt voor aanvallen met LockBit-ransomware*, 2021, https://www.security.nl/posting/715810/Australische+overheid+waarschuwt+voor+aanvallen+met+LockBit-ransomware, geraadpleegd op 9 augustus 2021.

[TECH2021], *Ransomware as a service (RaaS)*, 2021, https://whatis.techtarget.com/definition/ransomware-as-a-service-RaaS, geraadpleegd op 01 juli 2021.

[THAL2021], 2021 *Data Threat Report*, 2021, https://www6.thalesgroup.com/global/dtr/ppc/ty, geraadpleegd op 1 mei 2021

Kunter Orpak CISSP, CISA, CIA, ISO27001LA, CSX-F, CFSA, CCSA | Senior toezichthouder bij *de Autoriteit Financiële Markten*

Kunter Orpak werkt bij de Autoriteit Financiële Markten als senior toezichthouder op het gebied van operationele en ICT-risico's, waaronder informatiebeveiligingsrisico's. Hij is voornamelijk actief in het toezicht op de kapitaalmarkten. Kunter heeft meerdere jaren ervaring als interne auditor bij verschillende financiële instellingen. Kunter is lid van IIA Nederland en ISACA NL Chapter.