Hogeschool van Amsterdam

Ransomware

Auteur: Mahmoud Rashid
Docent: Bas Meyberg & Annelies Heek

Vak: IT Security
Datum: 12-10-2022
Versie: 2

Inhoudsopgave

Inleiding

Dit onderzoek bedoeld voor eerstejaars Cyber Security studenten, Middels dit onderzoek wordt antwoord gegeven op de volgende centrale onderzoeksvraag:

In hoeverre beïnvloedt de ransomware op mensen en bedrijven en hoe te beschermen tegen een ransomware aanval ?

De dreiging van ransomware neemt al jaren wereldwijd toe. Deze schadelijke software kan elk bedrijf schaden dat niet de juiste actie heeft ondernomen. De afgelopen jaren is er een nieuwe trend ontstaan: tegenstanders voeren meer gerichte ransomware-aanvallen uit op doelen die een hoger losgeld kunnen betalen.
Bijvoorbeeld : Op donderdag 9 september 2021 werd RTL Nederland het slachtoffer van een ransomware-aanval. Cybercriminelen zijn onlangs offline gegaan en computers zijn hersteld. Uiteindelijk heeft RTL 8500 euro aan de aanvallers betaald (ANP, 2021).
Om de hoofdvraag van een antwoord te voorzien, zullen de volgende deelvragen onderzocht en beantwoord worden.

- Wat is Ransomware?
    1. Wat voor verschillende soorten ransomware-aanvallen zijn er?
    2. Hoe werkt ransomware?

- Wat is de impact van een succesvolle ransomware aanval?
    1. Welke impact heeft de ransomware op Individuen?
    2. Welke impact heeft de ransomware op organisaties?

- Hoe gaan we ons beschermen tegen ransomware?
    1. Welke maatregelen zijn er om ransomware aanval te voorkomen?
    2. Hoe te herstellen na een ransomware-aanval?

Deze vragen worden hieronder duidelijk uitgewerkt. Vervolgens wordt dit onderzoek afgesloten met een conclusie waarin de hoofdvraag wordt beantwoordt.

1. Ransomware in het algemeen

Ransomware is schadelijke software waarmee een hacker op de een of andere manier de toegang tot de essentiële informatie van een persoon of bedrijf kan beperken en vervolgens geld kan vragen om de beperking op te heffen. De meest voorkomende vorm van beperking tegenwoordig is het versleutelen van belangrijke gegevens op de computer of het netwerk, waardoor de aanvaller in wezen gebruikersgegevens of een systeem kan gijzelen. ransomware is een snel groeiende bedreiging voor persoonlijke en zakelijke gegevensbestanden. Versleutel bestanden op een geïnfecteerde computer en bewaar de sleutel om de bestanden te decoderen totdat het slachtoffer losgeld betaalt. Deze malware is verantwoordelijk voor honderden miljoenen dollars aan verliezen per jaar (Brewer,2016).
De ransomware heeft twee hoofdtypen: Crypto ransomware en Locker ransomware . Alle ransomware soorten delen dezelfde kernfasen : infectie, uitvoeren, encryptie en gebruiksmelding.

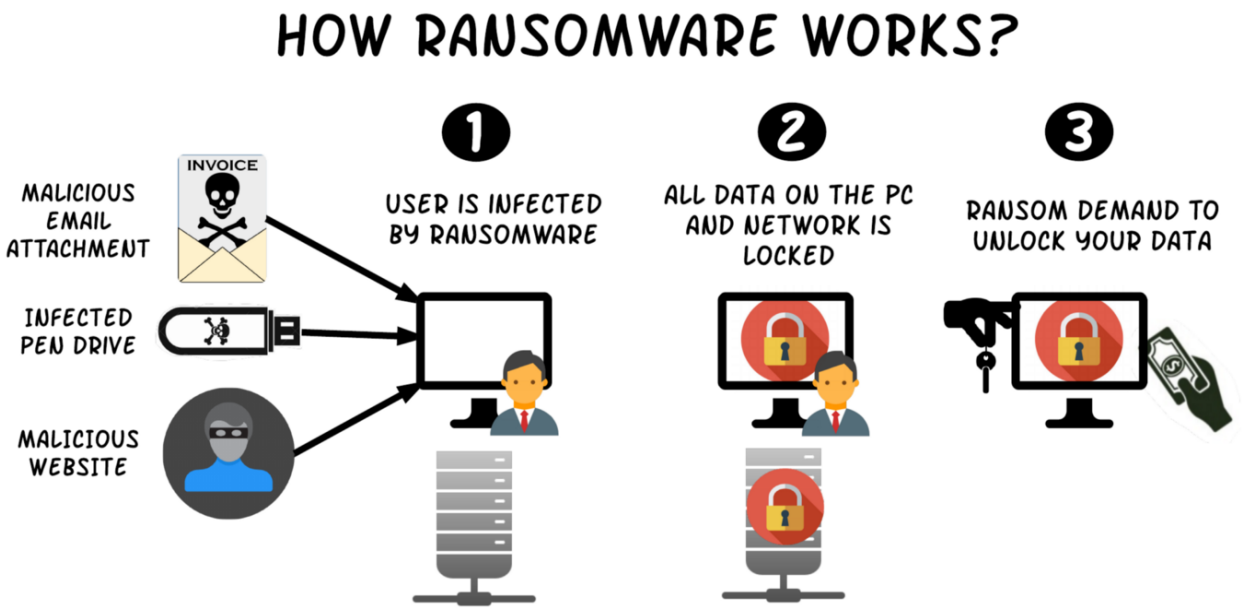
1.1 Ransomware soorten

Ransomware heeft verschillende soorten. Sommige onderzoekers beweren dat ransomware talloze varianten kent met 100 nieuwe vormen en patronen per jaar, andere onderzoekers spreken van twee hoofdtypen ransomware, in dit onderzoek zal ik me alleen concentreren op crypto-ransomware en locker-ransomware, die door verschillende onderzoekers en bedrijven worden beschouwd als de enige twee hoofdtypen van ransomware:

1. **Crypto ransomware:** Het doel van Crypto-ransomware is om uw belangrijke gegevens, zoals documenten, foto's en video's, te versleutelen, zonder de basisfuncties van de computer te verstoren. Dit kan paniek veroorzaken omdat gebruikers hun bestanden kunnen zien, maar er geen toegang toe hebben. Crypto-ontwikkelaars berekenen vaak hun losgeld vereisten: "Als u het losgeld niet binnen de deadline betaalt, worden al uw bestanden verwijderd." Omdat een groot aantal gebruikers niet weet dat er een back-up moet worden gemaakt naar de cloud of externe fysieke opslagapparaten, encryptie ransomware kan een groot effect hebben. Daarom betalen veel slachtoffers het losgeld alleen om hun bestanden op te halen (Kaspersky,2018).

2. **Locker ransomware:** Dit type malware verhindert de basisfuncties van de computer. Als de muis en het toetsenbord bijvoorbeeld gedeeltelijk zijn uitgeschakeld, kan de toegang tot het bureaublad worden geweigerd. Hierdoor kunt u blijven communiceren met het venster met het verzoek om losgeld om betalingen te doen. Anders kan de computer niet worden gebruikt. Maar het goede nieuws: Locker-malware richt zich meestal niet op kritieke bestanden, het wil je over het algemeen gewoon buitensluiten. Volledige vernietiging van uw gegevens is daarom onwaarschijnlijk (Giordano,2017).

1.2 Ransomware Werkwijze



https://miro.medium.com/max/1400/1*eeUhOlHKynIjgrpUtGm8Xg.png

Om succesvol te zijn, moet de ransomware toegang krijgen tot een doelsysteem, de bestanden daar versleutelen en losgeld vragen van het slachtoffer.
Hoewel implementatie details verschillen van de ene ransomware variant tot de andere, delen ze allemaal dezelfde kernfasen :

1. **Infectie**: aanvallers gebruiken technieken zoals social engineering en bewapende websites om te misleiden of te forceren gebruikers om een applicatie te downloaden die de infectie start.
2. **Uitvoeren**: Ransomware wordt geïnstalleerd en zorgt voor persistentie na een herstart – De ransomware zoekt naar bestanden om te encrypten op zowel de lokale computer als netwerkapparaten.
3. **Encryptie**: Ransomware voert een sleuteluitwisseling uit met de Command and Control Server, waarbij de coderingssleutel wordt gebruikt om alle bestanden te versleutelen die tijdens de uitvoering stap zijn ontdekt
4. **Gebruiksmelding**: er wordt een losgeldbrief gegenereerd, getoond aan het slachtoffer, en de hacker wacht om het losgeld te innen(Imperva,2021).

2. De impact van Ransomware

Het effect van ransomware op individuen is alleen betalen van losgeld maar niet-betalende slachtoffers hebben ook schade als zij tijdelijk of zelfs permanent niet meer bij waardevolle gegevens kunnen.Ransomware is niet alleen gericht op thuisgebruikers; bedrijven kunnen ook worden geïnfecteerd met ransomware, wat kan leiden tot negatieve gevolgen bijvoorbeeld:

- De normale bedrijfsvoering wordt onderbroken,
- Economische verliezen lijden door het herstellen van systemen en bestanden.
- Mogelijke schade aan de reputatie van de organisatie.
- Financiële druk kan leiden tot werknemers ontslaan.
- Bedrijfsgegevens, bedrijfsgeheimen en/of gegevens van uw klanten, medewerkers en of partners worden gelekt (Nfir, 2022b).

2.1 De impact van ransomware op Individuen

Ransomware heeft verschillende effecten op de economie. De betaling van losgeld is een maatschappelijk ongewenste herverdeling van geld van slachtoffers naar daders. Een dergelijke betaling is voor zover bekend beperkt tot een paar honderd euro per geval. Niet-betalende slachtoffers hebben ook schade als ze tijdelijk of zelfs permanent niet meer bij waardevolle gegevens kunnen.
Een onderzoek suggereerde dat de gemiddelde vraag om losgeld tussen 2014 en 2016 steeg van $ 294 tot $ 679. Het zou ons niet verbazen als de vraag om losgeld in de toekomst verder toeneemt. Een hoger losgeld betekent dat de welvaartskosten van ransomware zullen stijgen, en dus zal ransomware waarschijnlijk duurder worden voor de samenleving(Hernandez-Castro,2020).

2.2 De impact van ransomware op organisaties

Ransomware-aanvallen blijven groot worden en met een goede reden: op medium is er elke 11 seconden een nieuwe ransomware-aanval en organisatorische verliezen als gevolg van de aanvallen van ransomware wordt verwacht om in 2021 miljarden dollars in te bereiken, na een recordverlies van meer dan 225% in 2020.
Dus wat zijn de werkelijke kosten voor bedrijven die zijn getroffen door een ransomware-aanval?
Nieuw wereldwijd onderzoeksrapport van Cyber Eason onthult dat de overgrote meerderheid van organisaties die te maken hebben gehad met ransomware aanzienlijke zakelijke gevolgen hebben gehad, waaronder inkomstenderving, schade aan merk van onvoorziene personeelsverminderingen en zelfs de sluiting van
het bedrijf.
De belangrijkste bevindingen van het onderzoek zijn:

1. Verlies van bedrijfsinkomsten: 66 procent van de organisaties meldde een aanzienlijk omzetverlies na een ransomware-aanval.

2. Meer losgeld vragen: 35 procent van de bedrijven die losgeld betaalden, betaalde tussen $ 350.000 en $ 1,4 miljoen, terwijl 7 procent losgeld betaalde van meer dan $ 1,4 miljoen.

3. Merk- en reputatieschade: 53 procent van de organisaties geeft aan dat hun merk en reputatie zijn beschadigd als gevolg van een succesvolle aanval.

4. Ontslagen van werknemers: 29 procent meldde gedwongen te zijn werknemers te ontslaan vanwege financiële druk na een ransomware-aanval.

5. Bedrijfssluitingen: maar liefst 26 procent van de organisaties meldde dat een ransomware-aanval het bedrijf dwong om de activiteiten voor een bepaalde periode te sluiten(Curry,2021).

3. Beschermen tegen ransomware

Er is geen wondermiddel tegen ransomware-aanvallen. Ransomware is een van de vele varianten van malware. Daarom komen de acties die u tegen ransomware kunt ondernemen grotendeels overeen met de acties die u kunt ondernemen om uw systeem te beschermen tegen andere malware. Het doel van ransomware is meestal financieel gewin. Het is daarom aan te raden om je netwerk te beschermen met een in-depth verdedigingssysteem zodat kwaadwillende actoren extra inspanningen moeten leveren voor een succesvolle ransomware-aanval (Nationaal Cyber Security Centrum, 2021).

3.1 De maatregelen om ransomware aanvallen te voorkomen

De mens, of misschien beter (het gedrag van de mens): aanvallers maken veelvuldig gebruik van menselijk gedrag om voet aan de grond te krijgen. Zoals te verwachten, begint ongeveer 90% van een ransomware-aanval met een e-mail. Als we een e-mail ontvangen waarin we worden gevraagd iets te doen, hebben we de neiging om het meteen te doen.En de e-mail lijkt ook afkomstig te zijn van iemand die we kennen. Een collega. Regisseur. Een klant of familielid. Het adagium "Kijk voordat je begint" is in dit geval van toepassing. Denk na en controleer voordat u actie onderneemt. Hoe u op een link klikt of een bijlage opent. Controleer bij twijfel of alles correct is. Er zijn vaak genoeg aanwijzingen dat je eerst springt en dan denkt, waarom heb ik het niet gezien?(issys-ict,2020).

De technische maatregelen is eigenlijk preventie en detectie:

Preventie : De aanval is niet te stoppen, het is een feit. Voorkomen verwijst in dit geval naar het verkleinen van het aanvalsvak zodat de kans op succes van de aanval klein of niet is. Bijvoorbeeld door ervoor te zorgen dat kwetsbaarheden in onze systemen niet kunnen worden uitgebuit. Houd systemen en applicaties up-to-date met updates van leveranciers. Updates die zijn ontworpen om beveiligingsproblemen te dichten.

Detectie: Detecteren moeten we dan ook op verschillende manieren doen, ook moet er op verschillende plekken in de omgeving worden gedetecteerd. Zeker op plekken waar verbinding met onze systemen worden gemaakt. Denk aan een file- of mail server, website of clouddienst. Maar ook op systemen die aansluiten op onze omgeving. Zoals de computer waarop we werken of een mobiel apparaat.
Deze volgen over het algemeen de volgende 3 principes:

1. **Op basis van kenmerken:** Elke malware toepassing heeft specifieke kenmerken. Deze kenmerken kunnen we vastleggen in de database zodat we kwaadaardige applicaties gemakkelijk kunnen identificeren. Detection gebruikt een enorme database om de unieke kenmerken van malware vast te leggen. Dit betekent dat malware bekend moet zijn, dus we lopen altijd achter. De nieuwe malware moet immers eerst worden geïdentificeerd en de unieke kenmerken ervan worden toegevoegd aan de database. Dit is echter meestal de eerste stap bij het detecteren.

2. **Gedrag**: We kennen niet alle malware-applicaties, elke dag worden er nieuwe ontwikkeld. We kunnen het gedrag van malware herkennen omdat het eerder is gezien, of omdat het afwijkt van de norm. Als gevolg hiervan kunnen we toepassingen identificeren die worden uitgevoerd of proberen af te wijken van het verwachte gedrag en ze stoppen voordat ze schade aanrichten.

3. **Op misleiding gebaseerde detectie:** Misleiding is de derde techniek voor het detecteren van ransomware. Het meest voorkomende voorbeeld is het maken van een honeypot. Deze bestaande repository of server is het lokaas of lokaas voor de aanvaller. Gewone gebruikers zullen deze server niet aanraken, dus als hij activiteit ziet, is het waarschijnlijk een aanval(Johnson,2021).

3.2 Herstellen na een ransomware-aanval

Het onvermijdelijke is gebeurd en een of meerdere van uw bedrijfsmachines is geïnfecteerd geraakt. Wat doe je nu? Nu ga ik 6 stappen uitleggen :

1. **Betaal het losgeld niet**: Hoewel het verleidelijk kan zijn om het betalen van losgeld te beschouwen als de snelste manier om uw gegevens terug te krijgen, is er geen garantie dat de aanvallers uw bestanden daadwerkelijk zullen ontgrendelen zodra ze zijn afbetaald. Volgens de CyberEdge Group1 herstelt slechts 19 procent van de bedrijven die losgeld betalen, daadwerkelijk al hun gegevens en werkomgevingen, zoals beheerconsoles.

2. **Schakel alle apparaten uit en koppel ze los van het netwerk:** Zodra u de geïnfecteerde apparaten hebt geïdentificeerd, koppelt u onmiddellijk de netwerkkabel los, schakelt u wifi uit en sluit u die apparaten af. Veel soorten ransomware kunnen zich verspreiden via een netwerkverbinding, dus hoe eerder u de geïnfecteerde apparaten loskoppelt, hoe groter de kans dat u de inbreuk in bedwang houdt. Het is ook belangrijk om al uw gedeelde schijven tijdelijk offline te halen totdat u hebt vastgesteld dat alle geïnfecteerde systemen zijn geïdentificeerd. Blijf systemen controleren om vast te stellen of nieuwe bestanden versleuteld worden of verdwijnen.

3. **Zoek de bron**: Nu je maatregelen heeft genomen om de bekende schade in te dammen, zoek je jouw IT-omgeving naar aanwijzingen voor de bron. Elk systeem met verouderde of verkeerd geconfigureerde software wordt gemakkelijk gecompromitteerd. Neem contact op met al uw gebruikers om erachter te komen wie de eerste tekenen van de aanval heeft ervaren en wanneer. Was het nadat ze op een link in een e-mail hadden geklikt of kwamen er ongebruikelijke prompts uit hun webbrowser?

4. **Maak een nieuwe image van geïnfecteerde eindpunten, servers en virtuele machines:**
   Als een omgeving is geïnfecteerd, is er geen manier om te garanderen dat de ransomware volledig is verdwenen, tenzij je apparaten en virtuele machines schoonveegt en begint met een nieuwe image. Reimaging van de originele servers en applicaties zorgt ervoor dat ransomware is verholpen. In de tussentijd kan uw organisatie de bedrijfsproductiviteit nog steeds in beweging houden zonder onderbrekingen als u beschikt over een noodherstel plan voor de cloud, zodat uw organisatie kritieke applicaties en gegevens in VM's kan herstellen in een virtuele privé cloud.

5. **Herstellen van een back-up naar een schoon apparaat:** Nadat de schade is beperkt en u alle gebruikers op de huidige dreiging hebt gewezen om verdere infectie te voorkomen, is de beste manier om uw gegevens terug te krijgen zonder losgeld te betalen, deze te herstellen vanaf een opgeslagen back-up met een betrouwbare cloudservice zoals AWS. Met een geautomatiseerde back-up oplossing op bedrijfsniveau en de kennis van wanneer en waar de aanval plaatsvond, kunt u onmiddellijk teruggaan naar een niet-geïnfecteerde, in de tijd geïndexeerde momentopname van de gegevens van elk systeem. Moderne ransomware-pakketten maken gebruik van sterke bestandsversleuteling methoden zoals AES-128 of RSA-2048, waardoor het onmogelijk is om uw gegevens terug te halen zonder dat er een reservekopie beschikbaar is(Syntax,2021).

Conclusie

In de bovenstaande hoofdstukken hebben we gezien dat de ransomware verschillende typen heeft zoals:Crypto ransomware en Locker ransomware.
Bovendien hebben we gezien dat de impact van een ransomware-aanval is tegelijkertijd zeer groot voor individuen als bedrijven. Vervolgens wordt er duidelijk gegeven wat de technisch en niet-technische stappen om ransomware te voorkomen en in laatste hoofdstuk wordt duidelijk uitgelegd wat te do na een ransomware aanval.
Terug naar de hoofdvraag:
In hoeverre beïnvloedt de ransomware op mensen en bedrijven en hoe te beschermen tegen een ransomware aanval?
Op basis van de voorgaande hoofdstuk kunnen we zien dat de ransomware grote economische impact heeft op individuen en bedrijven en we hebben aangegeven hoe te beschermen tegen een aanval.

Aanbevelingen

In de afgelopen jaren zijn ransomware aanvallen toegenomen en ik denk dat het tijd is om nieuwe en effectieve beschermingsmethoden tegen ransomware aanvallen te bedenken. Bijvoorbeeld door een nieuwe detectie systemen te komen en het bewustzijn van mensen te vergroten om menselijke fouten te verminderen. Op deze manier kunnen we ransomware aanvallen verminderen en veel geld besparen.

.

https://studiostempel.com/wp-content/uploads/2017/12/icoon-idee.png

Bijlage I

Een uitgebreid research over cryptoware:

15. Ransomware, cryptoware en het witwassen van losgeld in Bitcoins

Een van de nieuwste ontwikkelingen op het terrein van cybercrime is ransomware. Dit is kwaadaardige software (malware) die toegang tot iemands computer en/of bestanden daarop blokkeert. Een specifieke vorm van ransomware is zogeheten cryptoware, die de bestanden versleutelt met behulp van cryptografie. Vervolgens eisen de cybercriminelen betaling van losgeld, vaak in de vorm van Bitcoins. Deze bijdrage gaat in op de vraag hoe cybercriminelen ransomware en cryptoware inzetten om geld te verdienen en hoe de verdiende Bitcoins vervolgens worden witgewassen.

Link naar het volledige research:
https://scholarlypublications.universiteitleiden.nl/access/item%3A3145345/view

Bijlage II

Een zeer interessante artikel over Behavior-based ransomware classification :

Abstract

Ransomware is malware that encrypts the victim's data and demands a ransom for a decryption key. The increasing number of ransomware families and their variants renders the existing signature-based anti-ransomware techniques useless; thus, behavior-based detection techniques have gained popularity. A difficulty in behavior-based ransomware detection is that hundreds of thousands of system calls are obtained as analysis output, making the manual investigation and selection of ransomware-specific features infeasible. Moreover, manual investigation of the analysis output requires domain experts, who are expensive to hire and unavailable in some cases. Machine learning methods have shown success in a wide range of scientific domains to automate and address the problem of feature selection and extraction from noisy and high-dimensional data. However, automated feature selection is under-explored in malware detection. This study proposes an automated feature selection method that utilizes particle swarm optimization for behavior-based ransomware detection and classification. The proposed method considers the significance of various feature groups of the data in ransomware detection and classification and performs feature selection based on groups' significance. The experimental results show that, in most cases, the proposed method achieves comparable or significantly better performance than other state-of-the-art methods used in this study for benchmarking. In addition, this article presents an in-depth analysis of the significance of various features groups and the features selected by the proposed method in ransomware detection and classification.

Link naar het volledige artikel:
https://www.sciencedirect.com/science/article/abs/pii/S1568494622001867

Literatuurlijst

ANP. (2021, 23 september). *RTL betaalde 8500 euro losgeld na cyberaanval*. Nieuws.nl. https://nieuws.nl/algemeen/20210923/rtl-betaalde-8500-euro-losgeld-na-cyberaanval/

Brewer, R. (2016, 1 september). *Ransomware attacks: detection, prevention and cure*. ScienceDirect. https://www.sciencedirect.com/science/article/abs/pii/S1353485816300861?casa_token=GwSxo0-x9lYAAAAA:hPirGxRoRDGzGTANxHVTPkMCbKu1wES87nE1ecDXJijypJClYhg4Si0Crf067Qw2VralUDxr

Curry, S. (2021, 16 juni). *Report: Ransomware Attacks and the True Cost to Business*. Cybereason. https://www.cybereason.com/blog/report-ransomware-attacks-and-the-true-cost-to-business

Giordano, S. (2017, 26 juni). *Know Your Ransomware Attacks Part I: Locker Ransomware*. cose.org. https://www.cose.org/en/Mind-Your-Business/Operations/Know-Your-Ransomware-Attacks-Part-I-Locker-Ransomware

Hernandez-Castro, J., Cartwright, A., & Cartwright, E. (2020, 4 maart). *An economic analysis of ransomware and its welfare consequences*. The Royal Society Publishing. https://royalsocietypublishing.org/doi/10.1098/rsos.190023#d3e1561

Imperva. (2021, 15 juni). *What is Ransomware | Attack Types, Protection & Removal | Imperva*. https://www.imperva.com/learn/application-security/ransomware/

issys-ict. (2020, maart). *De 5 meest gemaakte fouten in IT-beveiliging én tips voor een ijzersterke IT-beveiliging*. https://www.issys-ict.nl/wp-content/uploads/2020/03/security-gids.pdf

Johnson, K. (2021, 7 september). *3 ransomware detection techniques to catch an attack*. SearchSecurity. https://searchsecurity.techtarget.com/feature/3-ransomware-detection-techniques-to-catch-an-attack

Kaspersky. (2018, 7 augustus). *Cryptolocker Virus Definition*. Usa.Kaspersky.Com. https://usa.kaspersky.com/resource-center/definitions/cryptolocker

Morgan, S. (2021, 27 april). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Nationaal Cyber Security Centrum. (2021, 2 augustus). Ransomware. https://www.ncsc.nl/onderwerpen/ransomware

Nfir, S. S. C. U. |. (2022b, augustus 9). Wat voor impact heeft een ransomware aanval op mijn organisatie? Uw Cyber Security Specialist | NFIR. https://www.nfir.nl/wat-voor-impact-heeft-een-ransomware-aanval-op-mijn-organisatie

Syntax. (2021, 14 oktober). *10 Steps to Take After Falling Victim to a Ransomware Attack*. Syntax.Com. https://www.syntax.com/10-steps-to-take-after-falling-victim-to-a-ransomware-attack-2/