Aankondiging

# Webinar Ransomware

donderdag 14 oktober 2021

Ransomware, *hoe kun je het voorkomen en wat moet je doen wanneer het je overkomt?*

Ransomware (gijzel-software) behoort tot de grootste internetgevaren. Wat is het? Wat doet het? Hoe kun je je organisatie ertegen wapenen?
Ransomware heeft een enorme impact. Je kunt ongemerkt grote hoeveelheden bestanden, inclusief aangesloten back-ups verliezen. Criminelen richten zich steeds vaker op bedrijven en instellingen omdat daar veel geld te halen valt.

Peter van der Zwan, voorzitter van Stichting IP-Zorg, gaat hierover in gesprek met Jan Hanstege die zich hier binnen Z-CERT (Zorg-CERT) mee bezig houdt en met Ivo van Heerden, werkzaam bij een grote zorginstelling. Zij schetsen een beeld hoe hiermee om te gaan. Met volop tips en valkuilen uit hun eigen ervaring.

## Over de sprekers

### Jan Hanstede

Jan is werkzaam als security specialist bij Z-CERT. Hij houdt zich binnen Z-CERT bezig met digitale dreigingen. Hij ontwikkelt bijvoorbeeld het jaarlijkse dreigingsbeeld, schrijft whitepapers en spreekt op bijeenkomsten of webinars over cyberdreigingen. Daarnaast ondersteunt hij het operationele team bij *incident response* en bij het opsporen van kwetsbare systemen. Door zijn werk in de praktijk kijkt hij vanuit het perspectief van een hacker naar de zorg. Dit helpt om zorginstellingen weerbaarder te maken tegen cyberdreigingen.

### Ivo van Heeren

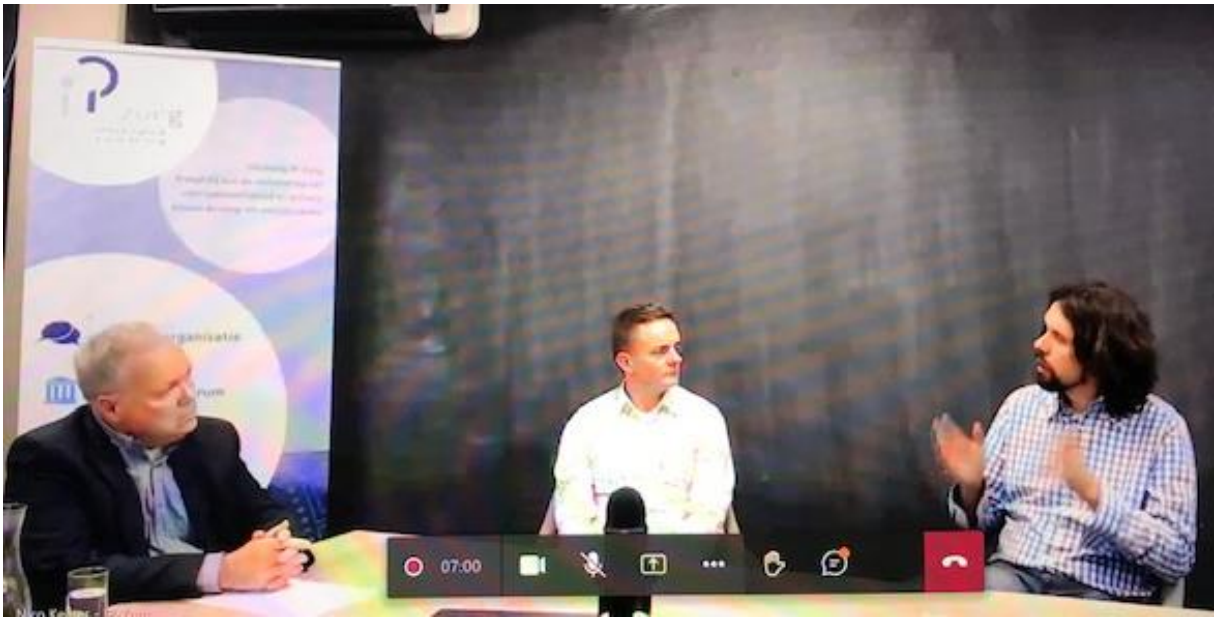
Ivo is werkzaam als Information Security Officer en Functionaris Gegevenbescherming bij Mijzo. Mijzo is een fusieorganisatie die op 1 januari j.l. is ontstaan uit de VVT-instellingen De Riethorst Stromenland, Volckaert en Schakelring. Voor de fusie was hij sinds eind 2017 voor alle 3 de organisaties al werkzaam als FG. In oktober 2020 is hij door de Raad van Bestuur benaderd met de vraag of hij ook de ISO-functie op zich zou willen nemen. Tot eind 2017 heeft hij ruim 17 jaar gewerkt als systeem- en netwerkbeheerder bij De Riethorst Stromenland. De laatste jaren kwam de nadruk steeds meer te liggen op gegevensbescherming en technische beveiliging.

Verslag

# Webinar Ransomware

donderdag 14 oktober 2021

*Het verslag is geen letterlijke weergave van de gesprekken. Wil je in detail weten wat er is gezegd en wil je de sprekers zien, ga dan naar het videoverslag of de podcast; het aangegeven tijdsverloop is daarbij behulpzaam.*




*Van links naar rechts: Peter, Ivo en Jan*

Peter opent het webinar en benadrukt de actualiteit van het onderwerp door te verwijzen naar de ransomware-aanval bij VDL waardoor de productie bijna een week stagneerde. Ransomware is een van de meest voorkomende en lucratieve uitingsvormen van hacking. Van een CIO is de uitspraak: er zijn 2 soorten organisaties: organisaties die zijn gehackt en organisaties die niet weten dat ze zijn gehackt. En wat doe je als je gehackt bent? Sluit je een cybersecurity verzekering? Keert die altijd uit? En wat moet een organisatie regelen voordat een verzekering wordt afgesloten? Is een ransomware aanval een verzekerbaar risico? Hoe staan de sprekers hierin?

4:00
Ivo stelt zich voor; zijn organisatie maakt zich grote zorgen om ransomware en noemt als voorbeeld De Mandemakers Groep waar de ict en telefonie plat hebben gelegen. Ivo benadrukt dat de risico's nog onvoldoende worden onderkend en dat ook de zorgsector een 'interessant' doelwit kan zijn. Mijzo heeft nog geen ervaring met ransomware . . .

6:00
Jan is bij Z-Cert verantwoordelijk voor het jaarlijkse dreigingsprofiel. Jan ziet een grote toename van ransomware, ook in de zorg. Hij noemt als voorbeeld Ierland waardoor centralisatie van patientsystemen 41 ziekenhuizen zijn geraakt door een ransomaanval met langdurige impact.
Jan noemt methoden om binnen te komen bij organisaties:

- Het massaal sturen van malware en afwachten tot iemand erin trapt . .
- Via RDP; een oplossing van systeembeheer om eenvoudig te kunnen inloggen in een windows-omgeving. Cybercriminelen proberen daarbij wachtwoorden uit om binnen te komen.

Dit maakt duidelijk dat multifactor authenticatie echt nodig is en dat je RDP niet direct aan het internet moet koppelen.

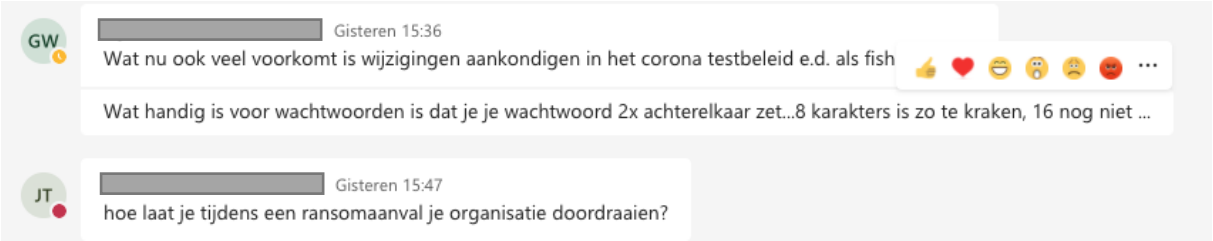
11:00
Peter vraagt Jan hoe hij de toename van ransomware verklaart .
Ca 2015 ging het nog om 1 hacker; daarna kregen we te maken met organisaties en nu wordt het een businessmodel. RAAS! Ransomware as a service!
Een dienstverlener die 'alles' regelt en een afnemer die alleen nog maar hoeft te hacken. De dienstverlener scant internet op zoek naar kwestbare toegangen om te verkopen aan hackers die data uiteindelijk versleutelen.

14:00
Wat kun je doen om Ransomware te voorkomen?
Ivo noemt uitvoeren patches, compartimentering (elke ingang naar het netwerk is een kwetsbaar punt), toezichthoudende domotica, standaard wachtwoorden, verplichte 2FA, zicht op wat er op het netwerk gebeurd (aanvallers zitten vaak langere tijd binnen en bereiden een aanval voor).
Kortom: "Je cyberhygiëne op orde hebben."

17:00
Jan noemt de 10 Gouden Tips om ransomware te voorkomen; zie website Z-Cert. https://www.z-cert.nl/wp-content/uploads/2021/02/Z-CERT_FactsheetRansomware_2560x1920px_04-1.pdf
Niet elke malware-aanval wordt door anti-virussoftware gedetecteerd. Je kunt aanvullende maatregelen treffen zoals in het netwerk 'aanzetten' welke programma's geactiveerd mogen worden met applicatie whitelisting en welke macro's mogen worden opgestart.

19:30
De rol van medewerkers is erg belangrijk. Medewerkers vertrouwen te veel op techniek. Ivo vertelt over de phising campagne die gedurende 9 maanden bij Mijzo heeft gedraaid; medewerkers moeten phising mails leren herkennen. Scan ook je eigen netwerkomgeving eens op eenvoudige wachtwoorden. Jan noemt een voorbeeld waarbij een scan op 'herfst2021' 5% score oplevert.
Bewustwording is een belangrijk punt. Gebruik je privé wachtwoorden niet zakelijk. Ivo benadrukt het belang van verplichte 2FA en single-sign-on.

25:30




Naar aanleiding van een chat adviseert Ivo wachtwoordzinnen te gebruiken; bij Mijzo zijn meer dan 10 characters verplicht én regelmatig wijzigen. Complexiteit eisen helpt niet.

Hoe ga je door als je geraakt bent?
Jan geeft aan dat dit afhankelijk is vanaf wanneer je het ontdekt. Een malware-infectie kan voorstadium zijn. Tools als end-point-detection en response-tools worden steeds vaker ingezet om hackers op te sporen.
Zit je in het eindstadium dan zit er vaak niets anders op dan een specialist in te huren.
Zou je bij Z-Cert zijn aangesloten dan kan Z-Cert je helpen met aangifte doen, met log-analyses, met second opinions. Z-Cert kan helpen maar doet geen specialistenwerk.

33:00
Hackers zijn vaak ook op zoek naar back-ups; zorg dat je die off-line hebt. Heb je dat niet dan zit er niets anders op dan te betalen.
Maar ook al heb je een goede back-up strategie; je weet niet wat een hacker doet met de buit-gemaakte informatie. Leidt dat tot datalekken? Tot reputatieschade?
Let op, cloud ontzorgt niet alles! Microsoft garandeert wel beschikbaarheid maar geen herstelbaarheid.


37:00
Stel dat je bent getroffen en het is echt mis; je bent data kwijt.
Jan stelt dat de beste strategie een zakelijke benadering is; je bent een van de vele! En doe het niet zelf, laat dat over aan een security-bedrijf.
Sommige ransomwaregroepen mijden de zorg; tast eerst af of dat misschien het geval is.

Ransomware aanvallen worden steeds efficienter; de gemiddelde 'doorlooptijd' is nu ongeveer 5 dagen. Ze kiezen vooral netwerken uit die voldoen aan bepaalde criteria. Een soort triage-slag.
Enige technische 'weerstand' regelen hoeft niet veel te kosten en is al snel effectief.

43:00
Mijzo heeft nog geen beleid voor ransomware; dit wordt een agendapunt voor directie-overleg. Een argument kan zijn dat, ook al heb je betaald en heb je je data terug, je nog niet weet wat daarmee is gebeurd.

45:00
Do's en don't?
Na een besmetting zoveel mogelijk afkoppelen en dichtzetten; ga de containerfase in om de rest van je netwerk te beschermen. Daar staat tegenover dat je bij forensisch onderzoek nu juist niet wil dat systemen zijn uitgezet; 'verkeersdata' moeten bewaard blijven. Wat je doet hangt af van de belangen; van de te verdedigen data.

47:00
Nog iets meer over de rol van Z-Cert.
Z-Cert is door de overheid aangesteld als Computer Emergency Response Team voor de zorgsector; het Nationaal Crisis Centrum kan gevoelige data met Z-Cert delen.
Z-Cert stuurt dagelijks advisory's over kwetsbaarheden; met gradaties van belang en risico.
Dit jaar 2x met zeer hoog risiconiveau met het advies om te updaten of te ontkoppelen.
Deelnemers die dat niet doen kunnen worden gewaarschuwd.
Daarnaast doet Z-Cert aan kennisdeling, white papers en webinars.
Deelnemers vormen een community en wisselen onderling ook informatie uit.
Z-Cert werkt wereldwijd samen met andere CERT-organisaties.

50:30
Mijzo is (nog) niet aangesloten bij Z-Cert; ze laat zich adviseren door een ethisch hacker.

Binnen VVT is te weinig expertise en wordt veel overgelaten aan externe partijen.
Z-Cert heeft een “ZorgDetectieNetwerk” voor zowel aangesloten zorginstellingen als de SOC-dienstverleners. Aangesloten instellingen delen hun ervaringen en bouwen zo een soort van collectief geheugen op. Dit is effectief omdat, afhankelijk van de sector, er vaak dezelfde leveranciers en systemen met dezelfde dilemma’s zijn.

57:00
De opmerking ‘we hebben alles in de cloud’ is geen excuus.
Jan noemt als voorbeeld een leverancier van een erp-systeem; werd geraakt door ransomware en bij 2 ziekenhuizen stagneerde het voorraadbeheer met ernstige gevolgen voor de patiëntenzorg. Met andere woorden, bevraag ook de leveranciers hoe die omgaan met ransomware-aanvallen. Een NEN 7510-certificaat zegt niet alles.

62:00
Jan benadrukt dat aangifte doen van een ransomware-aanval van belang kan zijn; ook de Politie investeert steeds meer in cyberveiligheid, ook internationaal. Informatie die als gevolg van aangiftes binnenkomt wordt gebruikt bij acties tegen cybercriminelen. Cybercriminelen lijken vooral vanuit de voormalige Oostbloklanden te opereren. Organisaties kunnen besluiten IP-adressen van bepaalde landen te blokkeren; maar cybercriminelen kunnen acteren vanuit waar dan ook.

68:00
Ivo gaat verder met presentatie van de Security Controls bij Mijzo, gebaseerd op het NIST Cybersecurity Framework. Sheets met toelichting zijn opgenomen in een apart document; ook beschikbaar via de website IP-Zorg.

78:00
Tot slot, naar aanleiding van een chat, de vraag hoe je tijdens een aanval de organisatie toch laat doordraaien. Belangrijk is dat je er vooraf over hebt nagedacht en draaiboeken hebt opgesteld. Wat zijn de herstelopties als je niet kunt terugvallen op je back-up; wat betekent gegevensverlies; wat betekent uitval van ict-systemen. En dat hoeft niet alleen door ransomware maar kan ook als gevolg van andere calamiteiten.

Peter sluit de bijeenkomst af; bedankt Ivo en Jan voor de constructieve bijdrage en overhandigt de bekende ‘IP-Zorg-beker met inhoud’.