



Piek ransomware-aanvallen op zorgsector Europa

De afgelopen weken zien de security analisten van Z-CERT een toename in het aantal cyberaanvallen op de Europese zorgsector. Meerdere zorginstellingen in België en Frankrijk zijn de hard geraakt door cybercriminelen die losgeld eisen. Ten aanzien van dezelfde periode vorig jaar is het aantal ransomware aanvallen op de zorg meer dan verdubbeld. Vooral nog is niet duidelijk waarom het aantal aanvallen nu zo piekt. Maar de ontwikkeling is voor Z-CERT genoeg reden om de Nederlandse zorgsector extra te waarschuwen.

18 februari 2021 | Malware

Van de volgende zorginstellingen is bekend dat zij de afgelopen weken zijn geraakt door ransomware.

- 28-12-2020 : Algemeen Medisch Lab ([België](#))
- 17-01-2021 : Ziekenhuis Chwapi ([België](#))
- 05-02-2021 : MNH: Franse zorgverzekeraar voor zorgpersoneel ([RansomExx](#))
- 09-02-2021 : Dax-Côte d'Argent hospital (Frankrijk) ([Egreqor](#))
- 11-02-2021: Dordogne ziekenhuis groep ([Frankrijk](#)) – 2 locaties besmet maar geringe impact
- 15-02-2021 : Ziekenhuis Nord-Oues ([Frankrijk](#)) (met impact op 3 locaties) (Ryuk)

Tien gouden tips tegen ransomware

De 10 belangrijkste maatregelen om ransomware incidenten te voorkomen of de impact te beperken.



- 1 Implementeer Applicatiewhitelijsting**
Definieer software en code die u veilig wilt uitvoeren op uw organisatie. Blokkeer de rest. Denk aan uitvoerbare bestanden, scripts, DLL's, modules, plugins en ook PowerShell.exe.
- 2 Stop of reguleer Office macro's**
Z-CERT raadt aan om macro's af te sluiten voor het internet met toe te laten. Pas toe het gebruik van macro's uit. Als dit (nog) niet kan, registreer het gebruik van macro's aan.
- 3 Patch applicaties en gebruik de laatste versies**
Geef in het patch management proces prioriteit aan de beheersaarden die voor zwaar de kans en impact tegen heeft zijn als High. Start het doel om deze binnen 10 uur te patchen.
- 4 Beveilig afstandsverlopingen**
Zorg ervoor dat afstandsverlopingen zoals Remote Desktop Protocol, TeamViewer en VNC niet onbeveiligd zijn aan het internet. Deze mogen alleen beschikbaar zijn via een beveiligde VPN of gelijkaardige oplossing.
- 5 Scan de buitenkant van uw IT-infrastructuur**
Scan regelmatig uw aan het internet verbonden systemen op afwijkingen en beheersaarden. Zoek HSP die onbeveiligd openstaan, of systemen die onbeveiligd toegankelijk zijn via het internet.
- 6 Beveilig uw applicaties**
Bijwerken check of u de beveiligingsupdates in uw systeem optimaliseert. Dit kan regelmatig functioneren bij. Controleer ook gebruikelijke functioneren met security checks uit, zoals CVE in Microsoft Office.
- 7 Pas least privilege principes toe**
Maak gebruik van een "least administration model" en geef geen bescherming rechten aan gebruikers. Geef alleen de rechten die noodzakelijk zijn voor de taken die de mensen uitvoeren (bijv. de toegang tot IT systemen). Systemen waar hoge rechten voor nodig zijn, mogen alleen uitgegeven worden vanaf "Privileged Access Workstations".
- 8 Maak regelmatig back-ups van belangrijke data**
Test het herstelproces regelmatig. Doe dit 3-2-1 regel toe en zorg ook voor offline back-ups. Systemen waarbij de back-up niet automatisch bewaard worden niet toegankelijk zijn met accounts die gebruikt worden voor andere systemen.
- 9 Patch de operation systems van uw apparaten**
Stel alleen versies van het operation system die ondersteund worden. Denk daarbij ook aan versies van embedded systemen die aan medische- en andere apparaten. Hierover geeft het artikel artikel 4.13 punt 3. Dit systemen die niet gepatched kunnen worden in een netwerkgevoelig andere van andere netwerk.
- 10 Implementeer multi-factor authenticatie**
Voor toegang tot online diensten en voor alle externe toegangssystemen tot uw IT-infrastructuur. Dit moet accounts en computers die toegang geven tot gevoelige data.

Z-CERT Stationsplein 121, 3818 LE Amersfoort www.z-cert.nl

Cybercrime

Mogelijk zijn meer zorginstellingen geraakt, maar is dat nu nog niet bekend gemaakt. Cyberspecialisten van Z-CERT gaan op basis van ingeziene informatie uit van georganiseerde cybercrime. Van een aantal incidenten is bekend welke ransomware-groepen erachter zitten, namelijk: Egregor, Ruyk en RansomExx. Dit zijn bekende cybercrime-actoren die al vele slachtoffers hebben gemaakt. Zo richtte Ruyk vorig jaar nog een ravage aan onder de [zorgsector in Amerika](#).

Dreigingsbeeld

In het onlangs gepubliceerde [Cybersecurity Dreigingsbeeld Zorg 2020](#) beschrijven securityspecialisten van Z-CERT de gevolgen van ransomware voor de zorg en de maatregelen die zorginstellingen kunnen nemen. Het is bekend dat cybercriminelen vaak standaardmethoden gebruiken om bij een organisatie binnen te komen. In onze handreiking '10 tips tegen ransomware' beschrijven we welke (preventieve) maatregelen de zorg kan nemen. Denk bijvoorbeeld aan het maken van back-ups. Deel deze handreiking binnen uw organisatie.

Techniek

Het wordt lastiger als de cybercriminelen eenmaal een organisatie zijn binnengedrongen. Het gaat hier om professionele cybercriminelen die acteren op een zeer hoog technisch niveau. We geven op onze website in een [serie artikelen](#) meer informatie hoe u uw detectie op een hoger niveau kan krijgen en deze cybercriminelen kan “vangen” in een detectieweb.