

Tien gouden tips tegen ransomware



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



1

Implementeer Applicatiwhitelisting

Definieer software en code die u veilig acht voor uw organisatie. Blokkeer de rest. Denk aan uitvoerbare bestanden, scripts, dll's, installers, packages en ook powershell.exe.



2

Stop of reguleer Office macro's

Z-CERT raadt aan om macro's afkomstig van het internet niet toe te staan. Faseer het gebruik van macro's uit. Als dit (nog) niet kan reguleren het gebruik van macro's dan.



3

Patch applicaties en gebruik de laatste versies

Geef in het patchmanagementproces prioriteit aan de kwetsbaarheden die voor zowel de kans en impact ingeschaald zijn als *high*. Stel tot doel om deze binnen 48 uur te patchen.



4

Beveilig afstandsworkoplossingen

Zorg ervoor dat afstandsworkoplossingen zoals Remote Desktop Protocol, Teamviewer en VNC niet ontsloten zijn aan het internet. Deze mogen alleen benaderbaar zijn via een beveiligde VPN of gateway-oplossing.



5

Scan de buitenkant van uw IT-infrastructuur

Scan regelmatig uw aan het internet ontsloten systemen op afwijkingen en kwetsbaarheden. Zoals RDP die onbedoeld openstaat, of systemen die onbedoeld toegankelijk zijn via het internet.



6

Beveilig uw applicaties

Bijvoorbeeld: check of u de beveiligingsopties in webbrowsers optimaal benut. Er komen regelmatig functionaliteiten bij. Schakel niet gebruikte functionaliteiten met security risico's uit, zoals OLE in Microsoft Office.



7

Pas least privilege principes toe

Maak gebruik van een "tiered administration model" en geef geen local-admin rechten aan gebruikers. Geef alleen die rechten die noodzakelijk zijn voor de taken uit te voeren gedurende tijd dat dit nodig is (JIT-admin oplossing). Taken waar hoge rechten voor nodig zijn, mogen alleen uitgevoerd worden vanaf "Privileged Access Workstations".



8

Maak regelmatig back-ups van belangrijke data

Test het herstelproces regelmatig. Pas de 3-2-1 regel toe en zorg ook voor offline back-ups. Systemen waarop de back-ups worden bewaard moeten niet toegankelijk zijn met accounts die gebruikt worden voor andere systemen.



9

Patch de operation systems van uw apparaten

Draai alleen versies van het operating system die ondersteund worden. Denk daarbij naast uw servers en desktopcomputers ook aan medische- en netwerkapparaten. Hiervoor geldt hetzelfde advies als bij punt 3. Zet systemen die niet geüpdatet kunnen worden in een netwerksegment achter een interne firewall.



10

Implementeer multi-factor authenticatie

Voor toegang tot online diensten en voor alle externe toegangsooplossingen tot uw IT-infrastructuur. Ook voor accounts en computers die toegang geven tot gevoelige data.