RANSOMEWARE BINNEN HET MKB

Ransomware is een groot probleem. Het slachtofferschap van ransomware heeft de afgelopen jaren een vlucht genomen. Door een laag bewustzijn en slecht beveiligde apparaten en netwerken zijn ondernemers een geliefd doelwit van cyber-criminelen. Het is daarom van belang dat alle ondernemers maatregelen nemen om zich tegen aanvallen met ransomware te beschermen. In deze folder lees je hoe.

In deze folder staan zes tips om jouwe bedrijf tegen ransomware te beschermen.

1. WAT IS RANSOMWARE

Ransomware is een vorm van cybercriminaliteit. Criminelen gebruiken software om de systemen of bestanden van je bedrijf onbruikbaar te maken door ze te versleutelen. Je kan dan niet meer op je apparaten komen, programma's gebruiken of je data zijn onbereikbaar geworden. Je bedrijf ligt dan dus helemaal plat. Via meldingen op je systeem wordt een flinke som losgeld gevraagd voor je weer toegang krijgt. Dit losgeld, of 'ransom', wordt meestal in crypto-valuta geëist door de cybercriminelen. Ransomware wordt ook wel gijzelsoftware genoemd.

Ook al betaal je het losgeld, is het altijd nog maar de vraag of je daadwerkelijk weer toegang krijgt. Soms betaal je wel, maar wordt er niets door de criminelen ontsleuteld. Of er volgt een nieuwe ronde van afpersing. Om extra druk te zetten om het losgeld te betalen dreigen de criminelen met het vrijgeven van buitgemaakte bestanden. Zoals kopieën van paspoorten van de eigenaar, of kwetsbare gegevens over de financiën van het bedrijf.

De kosten van zo'n incident kunnen al snel hoog oplopen. Het (eventuele) losgeld, korte termijn omzetverlies, langere termijn imagoschade en het herstellen van je systemen... 'Dat overkomt mijn bedrijf niet! Zo interessant zijn wij niet... Alleen grote bedrijven krijgen hiermee te maken'. Uit onderzoek blijkt dat bijna alle ondernemers dit denken. Wake up!

2. HET KAN OOK JOUW BEDRIJF OVERKOMEN!

Ondernemers die slachtoffer zijn geworden van ransomware, dachten namelijk net als jij: Dat overkomt mij niet! Toch loopt elk bedrijf een groot risico op aanvallen met ransomware: van online modewinkels tot garagebedrijven, van groot tot klein. Jazeker, ook jouw bedrijf loopt dit risico!

3. HOE WERKT RANSOMWARE

Er zijn veel manieren om bij jouw bedrijf binnen te komen en je systemen of bestanden te gijzelen. Hieronder de meest voorkomende ingangen die door criminelen gebruikt worden:

Wachtwoorden en accounts
• Toegegeven: het is best lastig om ingewikkelde en unieke wachtwoorden te gebruiken. We weten allemaal dat het belangrijk is en we doen het toch niet. Daar maken criminelen gebruik van om digitaal bij je bedrijf in te breken.
• Ook worden wachtwoorden buitgemaakt bij datalekken en vervolgens verkocht. Deze lijsten worden gebruikt door criminelen om in jouw systeem door te dringen.
• Maar tegenwoordig wordt ook geld geboden aan medewerkers van bedrijven om inloggegevens te verkopen aan criminelen.

Verouderde software
Elke software bevat zwakke plekken. In de updates van het programma, worden deze zwakke plakken vaak hersteld. Als jouw (beveiligings)software en apparaten niet draaien op de laatste versie, dan kunnen cybercriminelen gebruik maken van de kwetsbaarheden in de verouderde software om binnen te komen.

Phishing
Je hebt vast zelf ook wel eens een mailtje gehad dat er een pakketje voor je klaar ligt of dat je DigiD wordt geblokkeerd als je niet snel actie onderneemt. Phishingmails zijn vaak de eerste stap voor cybercriminelen om verder te komen in het netwerk van je bedrijf. Eenmaal binnen proberen ze om bedrijfsprocessen te blokkeren door het installeren van ransomware. Één medewerker is genoeg.

4. HOE BESCHERM IK MEZELF?

Het begint zoals we al aangaven bij sterke en unieke wachtwoorden. Dus doen; eventueel met behulp van een digitale wachtwoord-kluis. Dat is een programma waar je tegen betaling al je sterke en unieke wachtwoorden in kan maken en opslaan. Denk ook aan tweefactorauthenticatie. Gebruik dit, waar dit kan. Het stukje vertraging biedt je juist de veiligheid!
Het Digital Trust Center heeft speciaal voor ondernemers praktische tips ontwikkeld over veilig digitaal ondernemen. Er zijn ook ondersteunende tools. Hiermee kan je veel ellende voorkomen. (https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen).
Hieronder alvast in het kort een paar maatregelen.

QR Code

1. Maak back-ups
Als je bedrijf door ransomware wordt geraakt, moet je zoveel mogelijk data veilig hebben gesteld. Dus maak elke dag of elke week (automatische) backups die je liefst buiten het netwerk (bijvoorbeeld op een losse harde schijf, een NAS-server of liefst allebei) opslaat. Kleine moeite, maar je bedrijf kan vaak door als je door ransomware wordt geraakt. Je kan hier ook gespecialiseerde hulp en advies bij vragen aan cyber security bedrijven.

2. Inventariseer kwetsbaarheden
Hiermee beperk je de digitale risico's, en ben je goed voorbereid als je toch slachtoffer wordt. Stel jezelf de volgende vragen:
• Wat is de impact als het internet/systeem er 3 dagen, twee weken of een maand uitligt?
• Hoe erg is het als bepaalde gegevens op straat komen te liggen?
• Hoe erg is het als bepaalde gegevens niet meer kloppen?
Moeilijk om die digitale risico's in kaart te brengen? Nee hoor, op https://www.digitaltrustcenter.nl/tools/doe-de-basisscan-cyberweerbaarheid kan je een basisscan invullen. Doe het deze week nog!

3. Kies veilige instellingen
Kijk kritisch naar de instellingen van de apparatuur, software en netwerk- en internetverbindingen in jouw bedrijf. Standaardinstellingen zijn niet altijd het meest veilig dus deze kan je aanpassen. Het is ook belangrijk om goed te kijken naar functies en diensten die automatisch zijn ingeschakeld. Is dit wel echt nodig? Veiligheid gaat voor!

4. Voer updates uit
Door het installeren van updates worden kwetsbaarheden in apparaten en software hersteld. Zorg er dus voor dat updates automatisch worden geïnstalleerd, dan kost het je geen tijd. Zo draaien jouw (beveiligings)software en apparaten voortaan altijd op de laatste versie.

5. Beperk USB gebruik
Gegevensdragers zoals USB-sticks kunnen een systeem besmetten met malware. Ze worden soms op slinkse wijze je bedrijf binnen gebracht. Overweeg voor wie en wanneer USB-gebruik echt nodig is.

6. Beperk toegang
Niet iedereen heeft toegang nodig tot alle gegevens en systemen van een bedrijf. Bepaal dus per medewerker tot welke systemen en data toegang nodig is om haar/zijn werk goed uit te kunnen voeren. Verandert iemand van functie, pas de rechten dan aan.

7. Voorkom virussen en andere malware
Er zijn verschillende manieren waarop je virussen en malware kunt voorkomen: 1) veilig gedrag onder medewerkers stimuleren let daarbij vooral op het opnenen van bijlages en de dreiging van phishingmails, 2) een antivirusprogramma gebruiken, 3) apps veilig downloaden en 4) installatiemogelijkheden van software op apparaten van jouw onderneming beperken.

5. TOCH GETROFFEN DOOR RANSOMWARE?

Elk bedrijf loopt het risico om op een dag slachtoffer te worden van ransomware. Wees voorbereid, schaam je niet en kom in actie! Grote kans dat je niet precies weet wat je moet doen als je getroffen wordt. Kijk dan op: https://www.digitaltrustcenter.nl/informatie-advies/gehackt-wat-nu

Hieronder een aantal goede tips:

1. Maak een plan en bereid je voor op aanvallen met ransomware (uitleg hierover vind je op www.ncsc.nl). Print dit plan uit zodat het ook offline beschikbaar is.

2. Betrek in een zo vroeg mogelijk stadium van de aanval een IT-dienstverlener of een cybersecuritybedrijf, kijk nu vast of er een bedrijf bij jou in de buurt actief is of je online kan helpen, vraag eens onder welke voorwaarden ze werken;

3. Controleer zo snel mogelijk beschikbare back-ups op een niet-besmet apparaat en stel de back-up veilig. Sluit deze niet aan voor de bron van de besmetting duidelijk is.

4. Isoleer besmette netwerken, computers en apparaten. Haal ze uit het verdere netwerk en van het draadloze netwerk. Zorg er het liefst voor dat er geen digitale sporen verloren gaan: zet de apparaten niet uit en bewaar zoveel mogelijk informatie.

5. Bepaal vooraf wie kan en mag communiceren of eventueel onderhandelen met de aanvallers. Overweeg ook hierbij een externe professional als er een hoog bedrag wordt geëist.

6. Controleer op het ‘No More Ransom’ platform of er sleutels beschikbaar zijn voor het type ransomware dat je hebt.

7. Wijzig wachtwoorden van accounts die toegang hebben tot gevoelige gegevens en activeer waar mogelijk tweefactorauthenticatie.

8. Neem contact op de Autoriteit Persoonsgegevens als er ook sprake is van een datalek. Bij een ransomware-aanval, is de kans dat data is buitgemaakt en online rond gaat zwerven groot. Hier moet je melding van maken.

9. Meld de ransomware-aanval bij de politie of doe aangifte. Maak daarvoor een afspraak via 0900 - 8844.

10. Informeer medewerkers, klanten en medewerkers over wat er aan de hand is.

Wat als de enige optie is om de criminelen te betalen? Het kan zijn dat je besluit te betalen, omdat jouw bedrijf anders misschien wel failliet gaat. Er zijn bedrijven gespecialiseerd in het onderhandelen met cybercriminelen en het verzorgen van de betaling. Het is goed om in dit geval een expert te raadplegen en eventueel namens jou het contact te hebben met de criminelen.

Als je bedrijf slachtoffer wordt, maar ook wanneer je tot het besluit komt om criminelen te betalen, schaam je vooral niet! Het kan elke ondernemer overkomen. Erover praten helpt om anderen bewust te worden van dit risico en zich ertegen te beschermen.

Doe bij slachtofferschap van ransomware altijd aangifte bij de politie. Dat kost tijd maar met jouw aangifte weten zij wat er speelt, kunnen zij verdachten opsporen en help je andere ondernemers alert te zijn! Je kan de fraude ook online melden bij de Fraudehelpdesk. Zij kunnen dan andere ondernemers waarschuwen en zo veel ellende voorkomen.

Deze flyer is ontwikkeld in een samenwerking tussen het Veiligheidsnetwerk Oost-Nederland en het lectoraat Maatschappelijke Veiligheid van de Hogeschool Saxion, onder financiering van de Citydeal Lokale Weerbaarheid Cybercrime in samenwerking met het Centrum voor Criminaliteitspreventie en Veiligheid.