stichting carmelcollege

Let op: phishingmails en cryptolockervirus

Beveiliging van ICT-middelen blijft een belangrijk onderdeel van de werkzaamheden van de centrale ICT-afdeling van Carmel. Helaas is beveiliging nooit 100% gegarandeerd en daarom hebben we jullie hulp nodig.

Wat is precies het probleem?

De beveiligingsmaatregelen die Microsoft aanbiedt bij Ofice365, zorgen niet voor een 100% schone inbox. Soms kan dit omdat een virus of een van de andere gebruikte methodes te nieuw is. Soms kan het omdat een stukje software zoals waar het hier specifiek om gaat, een zogenaamde cryptolocker, in principe moeilijk te detecteren is omdat het voor een virusscanner lijkt op legitieme software. Er bestaat namelijk ook commerciële software met hetzelfde doel (het beveiligen van informatie op computers) en die ongeveer hetzelfde werkt. Dit maakt het opsporen van deze software ontzettend moeilijk en de afgelopen weken hebben we diverse keren een kleine en gecontroleerde uitbraak van dit probleem gehad.

Wat doet zo'n cryptolocker?

Cryptolockers doen precies dat wat de naam zegt; Bestanden worden versleuteld (en**crypt**ie) en zijn alleen nog beschikbaar voor de personen die de sleutel hebben, alsof de informatie in een kluis (**locker**) is geplaatst. Nadat het proces voltooid is, kan het bijna niet meer teruggedraaid worden, waar in het echt een kluis eigenlijk altijd nog wel opengemaakt kan worden met snijbranders, is dat bij cryptolockers niet meer het geval.
Na het versleutelen van de bestanden, wordt de computer opnieuw opgestart en zie je een melding als deze:

De criminelen hebben op dit moment volledige controle over je computer en je data. Alleen door het betalen van een som geld die tussen de € 100,- en € 5.000,- ligt wordt de computer weer vrijgegeven op afstand en kan je weer bij je bestanden.

Impact

In een netwerk van het formaat van de Stichting waar ruim 20.000 computers en duizenden servers met elkaar communiceren, komt er nog een vervelend iets bij; De cryptolocker zal ook alle informatie van alle computers die er gevonden worden versleutelen. Aangezien het versleutelen van bestanden niet als een abnormale actie gezien wordt (er wordt tenslotte op regelmatige basis gebruik gemaakt van versleuteling om extra beveiliging toe te voegen op de achtergrond), worden ook alle bestanden waar jij schrijfrechten op hebt versleuteld waarna ze onbruikbaar zijn. Voor een docent betekent dit dat veel data over bijvoorbeeld vaksecties niet meer leesbaar is, al het zelfontwikkelde digitale materiaal wat gedeeld wordt met collega's is voorgoed verloren. Voor teamleiders, die schrijfrechten hebben op grotere gedeeltes van de netwerken, betekent dit nog veel meer impact. Voor ICT-beheerders die overal rechten hebben…. Je begrijpt, dit is een zeer gevaarlijke situatie.

Wat is er aan te doen?

Bij het **kleinste beetje twijfel** of een mailtje wel of niet legitiem is, of een link wel of niet legitiem is, of een bij een mailtje gevoegd bestand wel of niet legitiem is, neem per direct contact op met de Helpdesk en verwijs naar deze communicatie. Ze zullen je vragen het mailtje door te sturen of nemen je computer op afstand over om mee te kijken. Klik in **geen enkel geval** op de link of het bijgevoegde bestand.
Op de achtergrond neemt de afdeling ICT maatregelen, alle binnenkomende email van externe personen zal niet meer direct naar Office365 gestuurd worden, maar komt binnen via gespecialiseerde mailscanners, waarmee alle email dus dubbel gescand wordt. Echter zoals eerder gezegd; beveiliging is nooit 100% te garanderen.

Een uitbraak…

Tot nu toe hebben we alle uitbraken kunnen terugdraaien. Laptops en computers van school worden simpelweg opnieuw geïnstalleerd, op geïnfecteerde servers zijn backups teruggezet. Het herstellen kost echter enorm veel tijd en soms is er om uiteenlopende redenen geen backup van de data, als de documenten bijvoorbeeld vandaag op het netwerk zijn geplaatst. Ook op deze vlakken wordt trouwens gewerkt aan meer inzicht, beveiliging en controle.

Ik heb geen Windows maar een Mac/Linux/ChromeOS/Chromium/BSD/OS/2,DOS, dus ik ben veilig!

Er zijn diverse effectieve cryptolockers in het wild aangetroffen die zich niets aantrekken van je besturingssysteem. Tevens richten criminelen zich op grote hoeveelheden van een verkocht iets. Op dit moment maakt de Mac-wereld ongeveer 10% uit van het totaal aantal gebruikte computers, maar in alle recent verkochte apparaten is dat aandeel veel groter (tot wel 40%). Hetzelfde geldt voor andere apparaten, het is tegenwoordig relatief eenvoudig om software van het ene naar het andere platform over te hevelen waarmee ons leven maar ook dat van de criminelen makkelijker wordt.

Leesvoer…

De Nederlandstalige Wikipedia heeft een lemma over ransomware, waar cryptolockers onder vallen: https://nl.wikipedia.org/wiki/Ransomware
De Engelstalige Wikipedia heeft een zeer uitgebreid lemma: https://en.wikipedia.org/wiki/Ransomware waarbij https://en.wikipedia.org/wiki/Ransomware#Encrypting_ransomware het ergste probleem omschrijft.

Meer informatie?

Voor meer informatie kun je mailen naar de contactpersoon Helpdesk/Servicedesk van jouw school.