CYBER AWARENESS
NASLAG

Versie 1.3
22 november 2019
Hoogeveen, T.B. (Thomas)

JJJJ

KKMMKLMLL

Webdexter®

Inhoudsopgave

1. Ransomware

Ransomware is computermalware die de toegang tot uw pc beperkt of zelfs volledig blokkeert of uw bestanden versleutelt. Vervolgens wordt geprobeerd om u een 'ransom' ofwel losgeld te laten betalen om weer toegang te krijgen.

Uw pc kan op de volgende manieren geïnfecteerd worden door ransomware:

- Onveilige, verdachte of valse websites bezoeken.
- E-mailberichten en -bijlagen openen die u niet had verwacht of die afkomstig zijn van personen die u niet kent.
- Het openen van schadelijke of onbetrouwbare koppelingen in e-mailberichten of berichten op Facebook, Twitter en andere sociale media of in chatberichten van Instant Messengers zoals Skype.

U kunt een vals e-mailadres of een valse webpagina vaak herkennen aan de slechte spelling of vreemde opmaak. Let op de onjuiste spelling van bedrijfsnamen (zoals 'PayePal' in plaats van 'PayPal') of ongebruikelijke spatiëring, symbolen of leestekens (zoals 'iTunesCustomer Service' in plaats van 'iTunes Customer Service').

Ransomware kan zich richten op elke pc, van thuiscomputers tot pc's in een bedrijfsnetwerk of servers die worden gebruikt door een overheidsinstelling.

2. Datalek in het geval van ransomware

De Autoriteit Persoonsgegevens (AP) krijgt geregeld vragen over datalekken waarbij ransomware of cryptoware is aangetroffen. Moet een organisatie dit melden aan de AP? Moeten betrokkenen, de mensen van wie de persoonsgegevens zijn, worden geïnformeerd? En wat kan een organisatie doen nadat een aanval is vastgesteld? De AP heeft als onderdeel van de campagne Alert Online informatie over ransomware en datalekken op haar site geplaatst.

Datalek
Als ransomware bestanden heeft versleuteld die persoonsgegevens bevatten, is dit een datalek. Er moet namelijk toegang tot de bestanden zijn geweest om deze te kunnen versleutelen.

De verantwoordelijke kan er bij ransom- of cryptoware niet van uitgaan dat de inbreuk beperkt is gebleven tot het zichtbaar besmette bestand of systeem. De besmetting kan het hele systeem en alle gekoppelde bestanden raken.

Er kan dus toegang zijn verkregen tot veel meer persoonsgegevens. Ook kan er meer met de gegevens zijn gebeurd dan op het eerste gezicht lijkt. De gegevens kunnen bijvoorbeeld zijn gekopieerd of gemanipuleerd.

Omvang inbreuk
Om de daadwerkelijke omvang van het datalek te bepalen, zal de organisatie onderzoek moeten doen. Hiermee kan de verantwoordelijke bepalen tot welke persoonsgegevens onbevoegde toegang is geweest en of de gegevens bijvoorbeeld zijn verkocht.

Als een verantwoordelijke geen onderzoek doet, moet hij ervan uit gaan dat alle gegevens in gekoppelde bestanden of systemen door de besmetting getroffen kunnen zijn.

Melden Autoriteit Persoonsgegevens
Bij inbreuken op de beveiliging waarbij ransomware is aangetroffen, gelden dezelfde criteria voor het melden van het datalek als voor datalekken met een andere oorzaak.

Dit houdt in dat organisaties (zowel bedrijven als overheden) het datalek bij de Autoriteit Persoonsgegevens moeten melden als dit leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Of als een aanzienlijke kans bestaat dat dit gebeurt.

Informeren betrokkenen
Organisaties moeten de betrokkenen in sommige gevallen ook informeren over het datalek. Dit moet als het datalek waarschijnlijk ongunstige gevolgen heeft voor hun persoonlijke levenssfeer.

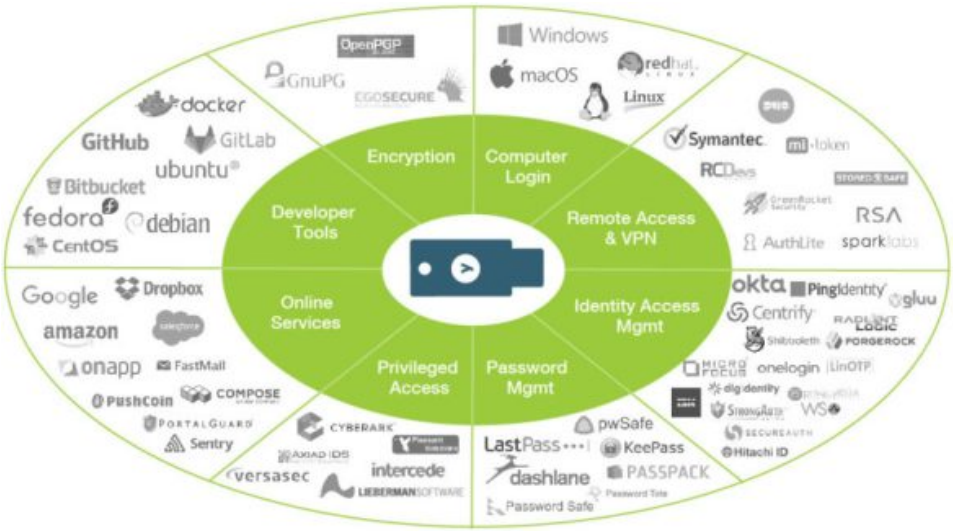
3. 2FA (Twee Factor Authenticatie)

Een gebruikersnaam en wachtwoord om aan te melden op een website of app, is dat anno nu nog veilig? Kort door de bocht: nee! Het is een kwestie van goed, beter, best. Toch hoort enkel een gebruikersnaam en wachtwoord niet meer thuis in dit rijtje. Het gebruik van een beveiligingssleutel is een oplossing om een extra laag beveiliging toe te voegen.

Samengevat is het tijd voor de inzet van Twee factor Authenticatie of Multi Factor Authenticatie, afgekort 2FA en MFA. Door middel van een dergelijke oplossing voegt u een extra beveiligings laag toe aan het aanmelden. Zo is het mogelijk om een bericht op je smartphone te ontvangen, een unieke code te gebruiken via Google Authenticator, of u kiest voor een fysieke beveiligingssleutel. De YubiKey is zo'n beveiligingssleutel.

Een Yubikey maakt het mogelijk om de tweede factor te zijn in het aanmelden. U voert uw gebruikersnaam en wachtwoord in en vervolgens verifieert u dat u het bent door de Yubikey in uw computer te stoppen en hem met uw vinger te activeren. Op deze manier weet het systeem dat een mens het proces activeert en niet een hacker op afstand en wordt de combinatie van uw accountgegevens en Yubikey gebruikt voor het aanmelden. Het voordeel is dat iemand nu wel uw wachtwoord kan raden of achterhalen, maar nog altijd de beveiligingssleutel nodig heeft. En die heeft u in handen.

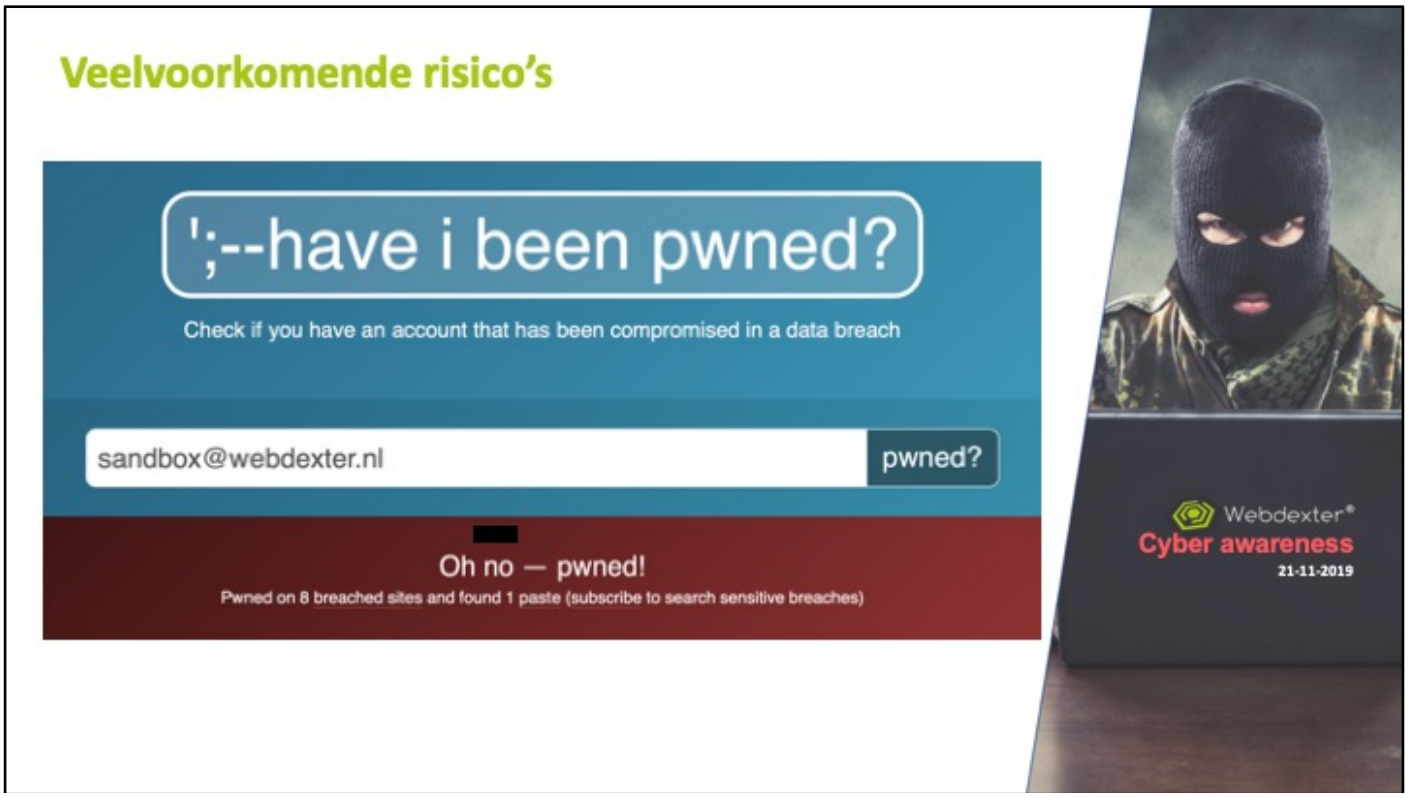
Er zijn inmiddels veel verschillende platformen die het aanmelden op basis van een beveiligingssleutel ondersteunen. Neem als voorbeeld Microsoft Windows en Apple MacOS. De beveiligingssleutel zorgt in dit geval voor de tweede factor bij het aanmelden op je computer. Een andere optie is het koppelen van de Yubikey op websites als Google, Facebook en Twitter. Ook tools als LastPass, Keypass en Dashlane ondersteunen de sleutel. U schaft hem dus eenmalig aan maar gebruikt hem op diverse platformen.



Onder andere verkrijgbaar bij Bol.com.

4. Have I been pwned!?

Via de website http://haveibeenpwned.com kunt u gemakkelijk controleren of uw accountgegevens voorkomen in een datalek. U kunt dit doen door uw e-mailadres in te vullen, vervolgens zal er worden gekeken of deze voorkomt in een database welke gelekt is. Indien uw e-mailadres bekend is in een datalek is het verstandig om spoedig uw wachtwoorden aan te passen.



5. DNS Security

Tijdens de informatieavond van Univé op 21 november is er diverse malen gesproken over DNS-security. In dit hoofdstuk vindt u meer informatie over dit onderwerp.

Wilt u een bepaalde internetpagina bezoeken, dan typt u simpelweg de domeinnaam (bijvoorbeeld google.nl) in de adresbalk van de webbrowser (bijvoorbeeld Internet Explorer) waarna de website 'vanzelf' wordt geopend. Het openen van een website lijkt misschien niets meer om het lijf te hebben dan het ophalen van de op een webserver opgeslagen bestand, maar in de praktijk ligt dat toch iets ingewikkelder. Het communicatieprotocol (dat wordt gebruikt voor de communicatie tussen browser en webserver) moet namelijk eerst zien te achterhalen op welke webserver een website wordt gehost. Het protocol kan echter niet overweg met domeinnamen, het is dus noodzakelijk deze eerst te vertalen naar het IP-adres van de server (een IP-adres bestaat uit 4 getallen uit de reeks 0-255, gescheiden door punten; bijvoorbeeld 172.217.168.227 voor de domeinnaam google.com).

Voor deze vertaalslag zijn alle domeinnamen met bijbehorende IP-adressen in een database opgeslagen welke toegankelijk wordt gemaakt via zogenaamde DNS-servers (DNS staat voor Domain Name System). Met het bij de DNS-server opgevraagde IP-adres kan het communicatieprotocol vervolgens contact leggen met de webserver van de betreffende website zodat deze in de browser kan worden geopend. Door de eigenaar van de DNS-server worden overigens altijd twee IP-adressen verstrekt waarvan er één als voorkeurs-DNS-server kan worden ingesteld en de andere als alternatieve DNS-server (is de voorkeurs-DNS-server overbelast dan kan het communicatieprotocol altijd nog gebruik maken van de alternatieve DNS-server).

Uw internetprovider levert u standaard DNS-server adressen aan waarin de eerste zoekslag plaatsvindt en de eventuele verwijzing. Vaak betreffen dit ongecontroleerde DNS-servers. Voor de veiligheid van endpoints (computer, laptop, smartphone etc.) is het verstandig om DNS-security toe te passen. In het geval van DNS-security worden de DNS-adressen in uw router aangepast en gekoppeld aan een uitgebreide database waarin ook dreigingen zijn opgenomen. Wanneer een endpoint connectie probeert te maken met een dreiging zal dit automatisch worden geblokkeerd. DNS-security versleuteld alle DNS aanvragen en scant deze op legitimiteit, zodra een apparaat connectie maakt met een onveilige website, dienst of server zal deze worden geblokkeerd. Binnen uw DNS-omgeving kunt u zien waarom en hoe een bepaalt adres en/of aanvraag is geblokkeerd.

Voor meer informatie over DNS-security kunt u contact opnemen met Webdexter via security@webdexter.nl.

6. Handige links

Rijksoverheid over Cyber Security
https://www.rijksoverheid.nl/onderwerpen/cybercrime

Nationaal Cyber Security Center
https://www.ncsc.nl

Diverse whitepapers over Cyber Security
https://www.ictwhitepapers.nl/security

Test uw security skills
https://www.alertonline.nl/cyberskillstest#/

Autoriteit Persoonsgegevens
https://autoriteitpersoonsgegevens.nl

Alles over ransomware
https://nl.malwarebytes.com/ransomware/

Politie over ransomware
https://www.politie.nl/themas/ransomware.html

Internetoplichting
https://www.politie.nl/themas/internetoplichting.html

Controleer of uw e-mailadres voorkomt in een gehackte database
https://haveibeenpwned.com

Sandbox voor Windows
https://www.sandboxie.com

7. Contactgegevens

Webdexter
Stadhoudersmolenweg 54C
7315 GJ APELDOORN

055-3034970

Thomas Hoogeveen
Thomashoogeveen@webdexter.nl
06-34143310

linkedin.com/in/thomashoogeveen/
@Webdexter.nl