
# WHITEPAPER

## ENDPOINT BEVEILIGING. OF HOE U DE DEUR NAAR UW DIGITALE APPARATEN OP SLOT DOET.

**De wereld om ons heen wordt met de dag smarter en we zijn in groeiende mate afhankelijk van digitale apparatuur. Met deze nieuwe digitale technologieën komen er nieuwe, digitale gevaren. Want met de groeiende afhankelijkheid van deze nieuwe technologieën worden we steeds kwetsbaarder. Als bedrijf en als persoon.**

# WHITEPAPER

## ENDPOINT BEVEILIGING. OF HOE U DE DEUR NAAR UW DIGITALE APPARATEN OP SLOT DOET.

Onze digitale veiligheid is in de afgelopen tijd vooral in het nieuws omdat, zo lijkt het, het ene na het andere bedrijf gehackt wordt. Maar een hack is niets meer dan een illegale inbraak op een computernetwerk en daarmee slechts een van de vele risico's die u loopt als gevolg van onze groeiende digitalisering.

Veel ondernemers denken dat het bij hun bedrijf zo'n vaart niet zal lopen. Waarom zou juist uw bedrijf gehackt worden? Daar heeft u deels gelijk in, alleen door de hype rondom cyber security zouden we bijna vergeten dat uw digitale veiligheid afhankelijk is van een groot aantal andere factoren. U moet daarom maatregelen nemen om uw bedrijf hiertegen te wapenen.

**Wat is Endpoint Beveiliging?**

Een van de belangrijkste maatregelen die u kunt nemen om uw digitale weerbaarheid te vergroten, is Endpoint Beveiliging. Onder Endpoints verstaan we laptops, pc's, servers, handhelds, smartphones en tablets. Het doel van Endpoint Beveiliging is om de gegevens op deze Endpoints zo goed mogelijk af te schermen tegen bedreigingen, zowel proactief als actief. Met proactief bedoelen we het ondernemen van actie voordat er iets gebeurt en gaat verder dan preventie.

Het optimaal inrichten van effectieve Endpoint Beveiliging vereist in ieder geval de volgende maatregelen:

1. **Het zoeken naar afwijkend gedrag**

Om te monitoren wat er gebeurt op een bepaalde machine (Endpoint) is het nodig om antivirus- en antimalware software en DNS Protection te installeren. Deze programmatuur signaleert bijvoorbeeld wanneer er een programma start dat bekend staat als onveilig, wanneer een programma afwijkend gedrag zoals het zoeken naar verbinding met een onbetrouwbare locatie vertoont of wanneer meerdere bestanden

### WAAR DIENT U OP TE LETTEN?

De BrainCheck is o.a. opgesteld aan de hand van fouten die bedrijven regelmatig maken. Deze punten zijn van belang voor ieder bedrijf, ongeacht grootte of branche. Met de opkomst van cybercriminaliteit is men geneigd om, gedreven door paniek en publieke opinie, de nadruk hier op te leggen. Echter, voor een bedrijf dat zijn algehele digitale veiligheid goed op orde wil hebben, is het van belang deze top 10 punt voor punt door te lopen.

in korte tijd worden versleuteld. Met het ontdekken van dit afwijkende gedrag is het mogelijk om tijdig in te grijpen en de gewenste actie te ondernemen.

2. **Het dichten van lekken**

In bestaande programma's en operating systems van Endpoints (Windows of macOS) worden regelmatig lekken gevonden. Deze kwetsbaarheden, die een bedreiging voor uw digitale veiligheid zijn, worden opgelost d.m.v. een update, oftewel een Patch. Het is van belang dat deze Patches zo snel mogelijk na uitgifte worden uitgevoerd zodat er geen lek ontstaat. Bovendien zorgen bepaalde combinaties van programma's voor beveiligingslekken, wat het beveiligingsproces nog complexer maakt. Gedegen Patchmanagement, het continu monitoren van geïnstalleerde software en de laatste updates uitvoeren, bij voorkeur centraal gemanaged en beheerd, is daarom onontbeerlijk voor een goed beveiligde, digitale omgeving.

3. **Het slot erop met Encryptie**

Bij alle apparaten waar data op staan, kan worden ingebroken. Maar ook na het per ongeluk verliezen van een mobiele gegevensdrager kunnen gegevens openbaar worden. Door een slot op de data te zetten zijn de gegevens op een bepaald Endpoint niet bereikbaar. Dit gebeurt door Encryptie, het versleutelen van data. Door gebruik te maken van Encryptie zijn de gegevens versleuteld en niet leesbaar, tenzij ze bijvoorbeeld met een wachtwoord worden ontgrendeld. Bij diefstal of bij verlies van een gegevensdrager is de data zonder wachtwoord niet leesbaar, wat het met name voor laptops en externe opslagmedia een geschikte vorm van beveiliging maakt.

**De moraal van dit verhaal**

Het slachtoffer worden van een hack is niet het enige of grootste digitale gevaar waar u in onze huidige digitale maatschappij tegenaan kunt lopen. Gelegenheid maakt ook de digitale dief en wanneer u de voordeur dicht timmert maar uw achterdeur wagenwijd open laat staan en uw apparatuur niet goed beveiligt, dan is het een kwestie van tijd voordat er iets misgaat met uw online beveiliging.

Zorg er daarom voor dat u uw Endpoints goed beveiligt, door middel van een passende oplossing. Wilt u hier meer over horen uit de mond van een expert? Maak dan een vrijblijvende afspraak met een van onze adviseurs via services@braincap.nl of bel naar **088-2754800.**

**Doe de BrainCheck**

Niet alleen Endpoints lopen een digitaal gevaar. Om u inzicht te geven in uw huidige niveau van digitale beveiliging en veiligheid, heeft BrainCap de BrainCheck ontwikkeld.

De BrainCheck behandelt een 10-tal punten die essentieel zijn met betrekking tot ICT-beveiliging en de veiligheid van de gegevens binnen een bedrijf en bestaat uit de volgende lijst van vragen en aandachtspunten:

- Back-up policy
- Gebruikersrechten
- Patchmanagement
- Wachtwoordpolicy
- Cloud Bestandsdeling en Synchronisatie
- Awareness
- Toegang van buitenaf
- Endpoint beveiliging
- Versleuteling van data
- Security Network Monitoring

Zegt niet alles u iets? Geen paniek, daar zijn wij voor. Nadat deze cruciale aandachtspunten besproken zijn, volgt er een rapportage met uw score op het gebied van digitale beveiliging en een aanbeveling. Met dit rapport kunt u zelf beslissen hoe u verdere invulling geeft aan een veilig ICT-beleid, waar we u uiteraard graag en vakkundig in adviseren. Neem contact met ons op via services@braincap.nl of bel ons op 088-2754800.

BRAINCAP
SOFTWARE & SERVICES