WHITEPAPER

HET DELEN VAN BESTANDEN. GEVAARLIJK GEMAKKELIJK.

De automatisering in bedrijfsleven en industrie biedt enorm veel voordelen, maar beseft u zich ook hoeveel risico's dit met zich meebrengt? Wilt u zeker weten in hoeverre u veilig bent, doe dan de BrainCheck. In deze whitepaper het gevaar van het delen van bestand. Enorm gemakkelijk. Maar met enorme risico's.

WHITEPAPER

HET DELEN VAN BESTANDEN. GEVAARLIJK GEMAKKELIJK.

Wanneer u enkele jaren geleden een presentatie nodig had voor bij een klant, bewaarde u deze op uw USB-stick. Inmiddels weet u wel beter. Gegevens meenemen op een USB-stick is fraudegevoelig en onveilig. U bent daarom gebruik gaan maken van FSS-oplossingen. Waarvan zegt u?

Wat is een FSS-oplossing

Een FSS (File Share and Sync) oplossing is een oplossing waarmee u gegevens beschikbaar maakt op een andere plek. Met andere woorden, oplossingen als Dropbox, OneDrive, Google Drive en Box, waarmee u op eenvoudige wijze bestanden deelt. Hetzelfde principe als de USB-stick, maar dan veel makkelijker. En met FSS-oplossingen kunt u nog veel meer. Wanneer u bijvoorbeeld DropBox niet alleen op uw pc maar ook op een andere pc, tablet of mobiele telefoon installeert, kunt u ook daar bij uw gegevens. Bovendien wordt iedere wijziging automatische gesynchroniseerd naar al deze apparaten én naar de mensen waarmee de gegevens gedeeld zijn. Daarmee is de meest recente versie overal en voor iedereen toegankelijk. Enorm handig en makkelijk dus en reden voor enorme populariteit van deze oplossingen. Maar zijn ze wel zo veilig?

Gevaren van het gebruik van FSS

Helaas is het antwoord op deze vraag ‘nee’. Weinig mensen zich realiseren dat juist bovenstaande functionaliteiten en het gebruiksgemak een groot aantal gevaren met zich meebrengt.

Ten eerste is er geen controle over waar de data terecht komen. Gebruikers die een FSS-applicatie installeren, krijgen automatisch toegang tot alle bestanden die in hun account beschikbaar zijn. Staat een bestand op een computer thuis, dan staat er ook een kopie van dit bestand op de pc op het werk, op de laptop en op een mobiel apparaat. Met andere woorden, een FSS-oplossing werkt als een digitale kopieermachine. Bovendien vergeet men na verloop van tijd waar welke informatie staat opgeslagen.

Worden gegevens dan ook nog eens met verschillende personen gedeeld, dan kunt u zich voorstellen hoeveel kopieën van data op plekken staan die niet meer te achterhalen zijn. Met de meeste FSS-

WAAR DIENT U OP TE LETTEN?

Onze 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, hier de nadruk 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.

oplossingen is dit niet te beheren en heeft de gebruiker zelf alle vrijheid, met alle risico's van dien. Want zeg nu zelf, hoe vaak brengt u in kaart waar u al uw bestanden heeft opgeslagen?

Iedereen een update. Van uw virus.

Ten tweede zit het gevaar in het feit dat iedere aanpassing van de gegevens automatisch overal wordt ge-update en iedereen daardoor de laatste versie heeft. Is een bestand beschadigd, bijvoorbeeld door ransomware, dan raken alle kopieën van dit bestand corrupt. De gehele stroom van gebruikers en machines waarop bepaalde data beschikbaar is, kan bestanden corrupt maken of corrupte bestanden ontvangen. Op deze manier raakt de volledige omgeving van alle gebruikers en machines besmet.

Hoe nu verder?

Voor uw bedrijf is het daarom van belang dat er een gedegen beleid wordt opgesteld om het gebruik van FSS-oplossingen in goede banen te leiden. Juist het gemak van de mogelijkheden die het gebruik ervan bieden, verlaagt de drempel om deze middelen in te zetten. Deze laagdrempeligheid vereist duidelijke regels en richtlijnen voor alle gebruikers. Bij het opstellen van een dergelijk beleid, dient u eerst antwoord te krijgen op vragen als: Welke data is toegankelijk en voor wie? Welke machines mogen een kopie van de data krijgen? Hoe zorgt u voor een goede back-up? Wat doet u bij verlies van data door diefstal of bij vertrek van een medewerker? Wie heeft er, op welk moment een of meerdere FSS-oplossingen geïnstalleerd? Heeft u inzicht in bovenstaande vragen, dan kunt u aan de hand daarvan een veilig beleid en beheer vaststellen.

Opties voor veilig FSS-gebruik

Om het gebruik van FSS-oplossingen zo veilig mogelijk in te richten en te beheren, zijn er diverse mogelijkheden beschikbaar. U kunt het gebruik zo inrichten, dat gegevens alleen voor een selecte groep mensen beschikbaar zijn. Dat gegevens alleen geïnstalleerd (en dus gekopieerd) mogen worden na goedkeuring van een beheerder. Of dat alleen apparatuur dat aan bepaalde eisen voldoet, zoals de een up-to-date antivirus/antimalware pakket, gebruikt mag worden.

Voor nu doet u er verstandig aan te inventariseren wat de status is van het gebruik binnen uw bedrijf. En om dit zo snel mogelijk dicht te timmeren. BrainCap Managed ICT Services heeft goede oplossingen beschikbaar voor de geschetste problemen en risico's, waar we u graag meer over vertellen.

Doe de BrainCheck

Niet alleen FSS-gebruik brengt menig digitaal gevaar met zich mee. 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 veilig ICT-beleid, waar we u uiteraard graag en vakkundig in adviseren. Neem contact met ons op via services@braincap.nl

BRAINCAP
SOFTWARE & SERVICES