WHITEPAPER GEBRUIKERSRECHTEN

WHO NEEDS ENEMIES...

Onze IT-omgeving staat bloot aan een groot aantal dreigingen. DDoS aanvallen zijn aan de orde van de dag en hackers proberen hun slag te slaan. Maar de grootste dreiging voor onze digitale veiligheid komt misschien wel van binnenuit. Namelijk door het misbruik of verkeerd gebruik van gebruikersrechten. Gewoon door eigen medewerkers.

WHITEPAPER

WHO NEEDS ENEMIES…

Als managed services provider zien we vaker dan ons lief is dat het goed regelen van gebruikersrechten bij veel bedrijven zwaar wordt onderschat. Met alle gevolgen van dien. Daarom bespreken we in deze whitepaper wat gebruikersrechten inhouden, hoe ermee om te gaan en vooral hoe te vermijden dat uw eigen personeel uw ergste vijand wordt. Vanuit de praktijk, zodat u er echt iets aan heeft.

Wat zijn gebruikersrechten?

Een gebruikersrecht is de autorisatie die een medewerker krijgt van de systeembeheerder op het gebruik van een (deel van een) systeem. Als we over gebruikersrechten spreken, dan hebben we het over:

1. De mate waarin medewerkers toegang hebben tot een systeem of systemen.

2. De mate waarin medewerkers toegang hebben tot de data op deze systemen.

3. In hoeverre medewerkers de mogelijkheid hebben om systemen te modificeren.

Deze drie aspecten bepalen het niveau van beveiliging en worden hieronder toegelicht.

Ad 1. Hoe bepaalt u de toegang tot het systeem?

Voordat gebruikersrechten kunnen worden toegekend, moet worden vastgesteld wie er toegang mag (of moet) hebben tot welk systeem. Dit geldt zowel voor de fysieke toegang als voor toegang tot het lokale netwerk of internet.

Er moet dus geregeld worden wie er waarbij mag komen. Dit kan op verschillende manieren ingericht worden, afhankelijk van de mate waarin de toegang beveiligd moet zijn. Hier volgt daarom een aantal voorbeelden om inzichtelijk te maken wat in de meest voorkomende situaties de beste oplossing is.

Thuiswerken

Een medewerker moet vanuit huis op een centrale server kunnen werken. Hiervoor zijn de volgende, veilige oplossingen beschikbaar:

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.

- De medewerker heeft toegang tot de server via internet op basis van het IP-adres. Een IP-adres is uniek per huishouden, waardoor dit een controleerbare en veilige oplossing is.

- De medewerker heeft toegang tot de server via een veilige VPN-verbinding. VPN staat voor Virtual Private Network en geeft de gebruiker beveiligde (versleutelde) en anonieme toegang tot een netwerk. Het maakt de internetverbinding veiliger en beschermt gegevens online.

Toegang tot Wifi op kantoor

Personeel en bezoekers van een kantoorpand moeten in dat pand toegang tot internet hebben. Allereerst moet er gekeken worden wie er van welk netwerk gebruik mag maken. Is het een medewerker van het bedrijf, dan kan hij of zij gebruik maken van het bedrijfsnetwerk. Het bedrijfsnetwerk geeft toegang tot centrale systemen, printers, e-mail en internet. Betreft het een bezoeker, dan mag hij of zij gebruik maken van een gastennetwerk. Een gastennetwerk is beperkt tot alleen e-mail en internet. Het is de meest eenvoudige en veilige manier om gasten toegang tot uw wifi-netwerk te geven.

Toegang tot de werkstations in het bedrijfsnetwerk

De gebruikers van een werkstation (een professionele computer voorzien van gespecialiseerde software en hardware) krijgen toegang tot het bedrijfsnetwerk door in te loggen met een gebruikersnaam en een wachtwoord* met een account. Op basis daarvan wordt bepaald of aan een account wel of geen toegang wordt verleend tot servers, printers etc.

Ad 2. Rechten op data

Wanneer iemand toegang heeft tot een systeem en is aangemeld, dan dienen er rechtenstructuren en een policy te zijn die regelen welke data zichtbaar, te modificeren of te verwijderen zijn. Data kunnen bijvoorbeeld wel te lezen zijn, maar niet aan te passen. Verder is het van belang dat indien nodig mappen en documentnamen zijn afgeschermd omdat de namen hiervan impliceren waar de inhoud over gaat. Een document met de naam Concept_Ontslagbrief_P_Jansen.docx kan weliswaar niet te openen zijn, de titel bevat al (vertrouwelijke) informatie over de inhoud van het document.

Ad 3. Het modificeren van systemen

Eindgebruikers van een systeem moeten documenten kunnen maken, lezen en aanpassen. Wat eindgebruikers niet moeten kunnen, is het aanbrengen van wijzigingen aan hun eigen of aan andere systemen. Dit kan leiden tot verstoringen of aanpassingen van toegangsrechten, met alle gevolgen van dien.

Het zodanig inrichten van de rechten van de gebruiker zodat hij of zij geen wijzigingen kan maken in het systeem, wordt, zo merken wij in de praktijk, het meest onderschat. Ook voor de gebruiker is het moeilijk om hier goed mee om te gaan. Want wanneer deze rechten niet naar behoren zijn ingericht, kan een gebruiker aanpassingen doen aan een van de systemen (pc, laptop, server, printer) en zelfs malware programmatuur opstarten. Doordat deze programmatuur automatisch de rechten van de gebruiker overneemt kan er nog veel meer schade ontstaan. Dit levert uiteindelijk extra belasting voor de IT-beheerder op.

Hoe worden de rechten bepaald?

Het is dus van belang om per gebruiker na te gaan welke rechten een medewerker nodig heeft en om het risico in te schatten waar het mis kan gaan. Bij het nemen van deze beslissing speelt de kennis van de eindgebruiker een rol. Want als deze zich niet bewust is van de gevaren, kan het verstandig zijn om de gebruikersrechten te minimaliseren en deze alleen bij uitzondering toe te kennen.

Heeft een werknemer eenmaal gebruikersrechten, dan moet worden bijgehouden of deze medewerker steeds dezelfde rechten moet blijven behouden. Met andere woorden, bij een functieverandering of uitdiensttreding moet er actie worden ondernomen. Procedures bij personeelsmutaties waarbij ook de beheerders worden betrokken zijn om deze reden essentieel.

Wie beslist er uiteindelijk welke rechten er aan welke medewerkers toegekend?

Op basis van wat er wel en niet is toegestaan moet er een duidelijk beleid vanuit het management worden opgesteld. Vervolgens kan Human Resources besluiten wie welke rechten nodig heeft, waarna tenslotte de beheerder de opdracht krijgt om functionaliteit en toegang toe te kennen of juist af te nemen.

Door gebruikersrechten strak in te richten, toegang selectief toe te kennen en alleen toe te staan tot wat nodig is, kunnen veel security issues en datalekken worden voorkomen. En daar zijn we ons op dit moment meer dan ooit bewust van.

*Het goed regelen van gebruikers- en toegangsrechten gaat hand in hand met de meeste andere punten uit de BrainCheck zoals wachtwoordbeheer, cloudbestandsdeling (FSS) en toegang van buitenaf.

Doe de BrainCheck

Om u inzicht te geven in uw huidige niveau van digitale beveiliging en veiligheid, heeft BrainCap de BrainCheck ontwikkeld. De back-up policy is hier onderdeel van.

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