Digital Security

2kmo01 | *Gaspard Nyssen* *Gilles Seyneave* *Remi Cloet* | *Group 11*

BeauPlace heeft veel personeel 'on the road' die een door het bedrijf verstrekte laptop gebruiken met standaard bedrijfs image.

Onlangs hebben meerdere incidenten plaatsgevonden

In onderstaande alinea's worden oorzaak en gevolg besproken en wat gezond is voor uw desktop/laptop

Wat kunt uw doen als een werknemer zijn paswoord werd gehacked.

De mogelijkheden om een gehacked wachtwoord tegen te gaan:

Als de hacker de trial and error heeft toegepast kan het bedrijf een Lockout inschakelen

- Oorzaak. Trial of error: methode waarbij men door krachtige computers te gebruiken zoveel mogelijk sleutels en paswoorden uitprobeer tot men toegangssleutel vindt die een encryptie breekt of toegang forceert

- Gevolg. Lockout. Dit zorgt ervoor na vele foute paswoord pogingen het systeem te sluiten zodat men niet meer kan inloggen. De hoeveelheid pogingen kan men zelf instellen. Ook de cooldown tussen de lockouts kan men zelf bepalen.

Voldoende uw computer updaten.

Gebruik maken van 'Password manager'. Deze genereert een master password. Dan hoeft u enkel deze te onthouden om toegang te krijgen tot alle andere accounts. Deze software kan een gemakkelijk en ingewikkeld wachtwoord maken zoals bv: 6ur7qvsZpb0ZkcuSW1u!V8ng!L^lb

Wat als uw laptop word gestolen en misbruik word gemaakt van uw facturen.

Voorzorgsmaatregelen voor uw data te beschermen bij diefstal zijn:

- Zorg ervoor dat elke werknemer zijn/haar desktop/laptop een gemiddeld tot moeilijk wachtwoord heeft.
- Gebruik wijzigingsinterval, bv om de 15 dagen, 1 maand, 2 maanden, … uw wachtwoord veranderen.
- Firewall doen wat het op ingesteld staat. Als een venster durft vragen voor toegang niet altijd 'oké' of 'akkoord' aanklikken
- Maak gebruik van IAM (identity and acces management sofware) kan er voor zorgen dat bv. De toegang tot uw account buiten de werkuren word geweigerd.
- Externe harde schijf
- Zorg voor back-ups bv een cloud.
- Een back-upstrategie, kan gemakkelijk zijn als voorzorgsmaatregelen.

Wat doen als een ontslagen werknemer interne dossiers meeneemt?

Het beste wat u hier kan doen is gebruiken maken van IAM

- Identity and acces management

Aan de hand van IAM kan je gelijk welk account uitsluiten en toegang weigeren tot uw data. Het profiel van de ontslagen werknemer sluiten. Wanneer deze persoon dan ook nog probeert aan te melden krijgt men een melding.

Standaard vitamines voor uw computer

- Laat binnen het bedrijf 1 zelfde merk rondgaan. Niet te veel variatie, dit zorgt voor kleine software verschillen waardoor sommige zaken anders worden gelezen. Ook gemakkelijk om reparaties uit te voeren
- Gebruik identity and acces management.

- Firewall
- Accepteer de updates die worden voorgesteld
- Voldoende automatische back-ups