SECURITY
MADEIN.LU

circl.lu cases.lu c-3.lu

Schaffe vun doheem : Sécher si virum COVID19 a sécher si viru Cyberkriminellen, déi virum Corona Virus net Halt maachen.

« Wien vun doheem aus ka schaffen, dee soll dat maachen. D'Sécherheet vun de Mënsche geet vir ! » Dat héiert een dëser Deeg zimmlech oft an et gëtt och ëmgesat. Mee bei all de Sécherheetsmoossname fir de Mënsch sollten d'Sécherheetsmoossname géint Cyberattacken am Kontext vun Teleaarbecht net vernoléissegt ginn.

Hei e puer Tipps fir sécher op Distanz ze schaffen.

Laptop & Co

- Gitt besonnesch gutt uecht, datt ären techneschen Equipement ewéi USB, Handy, Laptop an/oder Tabletten net gestuel,verluer oder vertässelt ginn.

- Vergewëssert Iech, datt all Apparat aktualiséiert ass, wéi den "operating system update" (iOS oder Android) an datt d'Software an Antivirus um leschte Stand sinn.

- Wann der mat sensibelen Date schafft, da passt op datt keen Iech op de Schierm ka kucken

- Späert Äre Computer wann der Är Plaz verloosst.

- Vergewëssert Iech, datt Äre Computer an all aner technescht Aarbechtsgeschier ausgeschalt, gespaart oder op enger sécherer Plaz verstaut ass, wann Dir se net benotzt.

- Benotzt sécher Zougangsmethoden, ewéi multi-factor Authentifikatioun a staark Passwierder a, wa méiglech, Encryptioun fir den Zougang zum Computer anzeschränken an de Risk ze minimiséieren, wann de Computer gestuel oder verluer gëtt.

- Wann e Computer (Tablet, Handy, Laptop) gestuel oder verluer gëtt, sollt Dir direkt reagéieren an d'Memoire op Distanz läsche kënnen.

Email

- Benotzt Är Aarbechts-Email-Adress an net Är privat fir berufflech Emaile mat perséinlechen Donnéeën ze verschécken. Wann Dir Äre privaten Email musst benotzen, da vergewëssert Iech, datt de Contenu an d'Attachementer verschlësselt sinn, an evitéiert datt perséinlech oder confidentiel Donnéeën am Betreff/Sujet/Subject stinn.

- Ier Dir Är Maile verschéckt, vergewëssert Iech, datt Dir se un dee richtegen Empfänger schéckt, zemools déi Maile mat perséinlechen a sensibelen Donnéeën.

- Wa nëmme méiglech, schéckt verschlësselt Mailen.

Cloud a Reseau Zougang

- Connectéiert Iech net op ëffentlechen an net bekannte Reseauën:

    - Connectéiert Iech op den 3G oder 4G Reseau wann der keen Zougang zu engem séchere WiFi hutt.

    - Benotzt VPN

- Wou méiglech, benotzt nëmme vertrauenswierdeg Reseauën an/oder Cloud Servicer vun Ärer Firma am Accord mat Ären interne Reegelen a Prozeduren fir den Zougang zur Cloud oder dem Reseau, fir de Login a 'Deele vun Donnéeën.

- Wann Dir ouni Zougang zu engem Réseau oder Cloud schafft, da suergt dofir, datt vun den Donnéeën, déi lokal gespäichtert ginn, reegelméisseg en adequate Back-up gemaach gëtt.

- "Remote access software", wéi Teamviewer, soll mat grousser Virsiicht an nëmme vun autoriséierten Employéeë benotzt ginn. Esou eng Software muss ëmmer aktualiséiert ginn a soll nëmmen an absolut dréngende Fäll genotzt ginn.

Speziell fir de CISO

- Vergewëssert Iech, datt all mobil Geräter déi vun den Employéeë benotzt ginn, geséchert sinn, an datt Dir d'Méiglechkeet hutt, fir se ze wipen am Fall wou se gestuel oder verluer ginn.

- Benotzt Mobile Device Management fir d'Geräter vun de Employéeën ze sécheren.

EN Version :
https://securitymadein.lu/news/covid-19-safety-and-cybersecurity-can-go-hand-in-hand/