Bescherm uw digitale en fysieke informatie

Voor velen is data wat olie vroeger was. Zakelijke online systemen en archieven, waar vertrouwelijke gegevens vaak zijn opgeslagen, zijn daarom in de ogen van cybercriminelen pure goudmijnen (of beter gezegd begeerlijke olievelden). Ze zullen er alles aan doen om daar in te breken.

Er worden dagelijks duizenden online systemen gecompromitteerd. Alleen al vorig jaar kreeg 39% van de bedrijven in heel Europa te maken met een cyberaanval[1]. Het aantal tot nu toe gerapporteerde gegevensinbreuken is dit jaar echter al hoger dan in heel 2020.

Als reactie daarop moeten bedrijven specialisten inzetten met de kennis van zaken en de instrumenten om uw vertrouwelijke informatie te beschermen. En onze essentiële gegevensbeschermingstips helpen u om precies dat te doen.

[1] Source: Statista

01

Een regeling voor het risicobeheer instellen

Met een regeling voor het risicobeheer kunnen bedrijven bedreigingen identificeren en begrijpen, en u daarna helpen met het elimineren of reduceren van deze risico's door de technologie, systemen en informatie in uw organisatie te beveiligen.

02

Beveilig uw netwerken

Essentiële elementen voor cyberbeveiliging zijn firewalls en antivirusprogramma's. Controleer legitieme e-mails: onder de waarschuwingssignalen dat er iets mis is vinden we spelfouten, slechte grammatica, merkwaardige formuleringen en spoedverzoeken om geld of om een bepaalde handeling uit te voeren.

03

Gebruik sterke wachtwoorden

Sterke wachtwoorden hebben acht tekens of meer en bevatten een combinatie van hoofdletters en kleine letters, getallen en symbolen. Bewaar wachtwoorden op een veilige plaats, gebruik hetzelfde wachtwoord niet voor meerdere accounts en verander ze om de drie maanden.

Wij beschermen wat belangrijk is.

Shred-it®
Een Stericycle®-Oplossing

04

Plaats minder op de social media

Cybercriminelen kunnen uw vertrouwelijke informatie met maar enkele datapunten verkrijgen, dus hoe minder u publiekelijk deelt, hoe beter! Als u bijvoorbeeld de naam van uw huisdier bekend maakt, kan het zijn dat u een antwoord prijsgeeft op een gangbare veiligheidsvraag.

05

Opleiding en bewustmaking van werknemers

Ontwikkel beleidsrichtlijnen voor de beveiliging en geef bewustzijnstraining over cyberveiligheid. Werknemers moeten weten hoe ze verdachte e-mails of links kunnen identificeren en moeten voorzichtig zijn met de websites die ze bezoeken en de applicaties en mobiele apps die ze downloaden. Moedig teams aan om alle cyberaanvallen te melden.

06

Gebruik vernietigingsservices voor de harde schijf

Zorg dat er niet te veel computers zijn of opeenhopingen van digitale data. Sla digitale gegevens op in bestanden en reinig die bestanden regelmatig. Als uw computertechnologie verouderd is, laat dan de oude of ongebruikte harde schijven veilig vernietigen.

07

Bescherm smartphones en andere apparaten

Mobieltjes en andere apparaten kunnen uw zwakke schakel zijn. Laat ze nooit onbeheerd achter en zorg dat ze wachtwoordbescherming hebben. Zorg dat uw mobiele apps en besturingssystemen up-to-date zijn en dat ze verloren of gestolen apparaten kunnen traceren, vergrendelen en wissen.

08

Vergeet niet dat ook fysieke documenten kunnen worden bedreigd!

Ook oude documenten vormen een aanzienlijk risico als ze niet veilig worden behandeld, opgeslagen en vernietigd. Een Clean Desk Policy kan de veiligheid ondersteunen, terwijl een Compleet Shred-it Beleid helpt met het verminderen van het aantal menselijke fouten die gegevensinbreuken veroorzaken.

Wij beschermen wat belangrijk is.

Shred-it®
Een Stericycle®-Oplossing