Mijn thuiswerksysteem is onveilig, wat nu?

RendementOnline

Door redactie FA Rendement

3 april 2023 | 6 minuten

Werknemers werken deels vanuit huis. Veilig thuiswerken is steeds belangrijker. Maar wat als het fout gaat? Ondanks uw voorzorgsmaatregelen is er toch sprake van een onveilige thuiswerkomgeving. Er is bijvoorbeeld sprake van een datalek. Of u verneemt uit de media dat uw thuiswerksysteem onveilig blijkt te zijn, waardoor mogelijk gevoelige gegevens op straat kunnen komen te liggen. Denk aan het incident bij softwarebedrijf Citrix begin dit jaar. Via een beveiligingslek konden computercriminelen informatie stelen of gijzelingssoftware installeren. Een ander recent voorbeeld is de discussie omtrent veiligheids- en privacy-issues bij videoconferentie-app Zoom.

Wat moet u eigenlijk doen als er sprake blijkt te zijn van een onveilige thuiswerkomgeving? Hieronder vindt u tips voor 4 situaties:

- een datalek bij uw eigen organisatie;
- een datalek bij de aanbieder van uw thuiswerksysteem;
- inbreuk op uw videomeeting door een onbevoegd persoon;
- negatieve mediaberichtgeving over uw thuiswerksysteem op het gebied van privacy of informatiebeveiliging.

In elk van deze situaties gelden namelijk dezelfde 3 stappen die u moet doorlopen.

1. De-escaleer

Als blijkt dat uw gegevens niet (meer) voldoende beschermd zijn, is het eerste wat u doet het de-escaleren van de aangerichte schade en tegelijkertijd het voorkomen van verdere schade.

Escaleren en de-escaleren

Volgens het woordenboek is escaleren het zich geleidelijk uitbreiden van een situatie. In een zakelijke omgeving bedoelen we hier doorgaans een bewuste handeling mee, die als doel heeft een probleemsituatie een groter belang te geven, zodat deze betere aandacht krijgt.

Een medewerker van de helpdesk kan bijvoorbeeld de melding van een grote IT-storing escaleren, zodat die bij een afdeling terechtkomt die beter in staat is de storing op te lossen.

De-escaleren
Het tegenovergestelde hiervan is de-escaleren. Hierbij probeert iemand juist de ernst van een situatie minder te laten zijn of lijken. Ook kan het betekenen 'de gemoederen tot bedaren brengen'.

Datalek eigen organisatie

Een datalek is een beveiligingsincident waarbij persoonsgegevens in handen van onbevoegden komen of waarbij persoonsgegevens onbedoeld verloren gaan. Een datalek kan dus de illegale inzage of toe-eigening van persoonsgegevens betreffen, maar ook het per ongeluk versturen van persoonsgegevens naar de verkeerde persoon, of het verloren gaan van persoonsgegevens zonder dat er sprake is van een back-up.

Als u een datalek waarneemt (of dit vermoedt), onderneem dan in ieder geval de volgende stappen:

- Artikel 33 van de Algemene verordening gegevensbescherming (AVG) verplicht organisaties om een datalek binnen 72 uur te melden aan de Autoriteit Persoonsgegevens. Zie ons voorbeelddocument Procedure Datalek en Beveiligingslek voor meer informatie.
- Informeer zo snel mogelijk de aangewezen persoon binnen uw organisatie.
  Dit kan de functionaris gegevensbescherming (FG) zijn of iemand van de ICT-afdeling.
  Raadpleeg bij twijfel uw leidinggevende.
- Bewaar het bewijs voor onderzoek naar het potentiële datalek.
  Het is belangrijk om te onderzoeken hoe het datalek heeft kunnen plaatsvinden en wat de daadwerkelijk aangerichte schade is. Dit onderzoekt u samen met de aangewezen persoon binnen uw organisatie. U herleidt het lek naar de bron, zodat deze gedicht kan worden.
- Naar aanleiding van het onderzoek moeten de juiste maatregelen worden genomen om het lek te dichten.
  Is het aantal betrokkenen bekend? Is er bekend om welk type persoonsgegevens het gaat?
- Indien nodig: melding maken bij de Autoriteit Persoonsgegevens (AP).
  Of het nodig is een melding te maken bij de AP hangt af van een risicoafweging die wordt gemaakt op basis van de ernst en de vermoedelijke gevolgen van de inbreuk. Als er opzettelijk data is gestolen (of u heeft dit vermoeden), doe dan aangifte bij de politie.

Datalek aanbieder

Het kan gebeuren dat een van uw aanbieders een datalek heeft.

- Is een eventueel datalek officieel bevestigd door de aanbieder van de dienst?
  Online gaan er vaak geruchten rond. Het is van belang om de aanbieder om bevestiging te vragen. De bevestiging geeft meer zekerheid en daarnaast wordt het ook duidelijk of het lek een impact heeft op de geleverde diensten.
- Zodra er bevestiging is van het lek, is het van groot belang om de dienst in ieder geval niet meer te gebruiken tot het verhelpen van het lek formeel is bevestigd.
  Bij het thuiswerksysteem Citrix werd in januari geadviseerd om de dienst niet meer te gebruiken en zelfs de stekkers volledig uit de servers te halen.
- Onderzoek naar – en het vaststellen van het potentiële lek.
  Onderzoek wat de daadwerkelijke aangerichte schade is. Wat is er gebeurd in de periode dat u met een onveilig systeem heeft gewerkt? Heeft het lek impact op uw bedrijfs- en persoonsgegevens?
- Neem het systeem pas weer in gebruik als er voldoende beveiligingsmaatregelen zijn getroffen door de aanbieder.
  Dit kan zijn door middel van een software-update of sterkere wachtwoorden.

Inbreuk videomeeting

Uw videomeeting blijkt onveilig want er is ingebroken in uw videomeeting.

- Verzamel bewijs, bijvoorbeeld door het maken van een screenshot of filmpje met uw mobiele telefoon.
  Zo is het gemakkelijker om naar de autoriteiten te stappen en deze persoon te identificeren.
- Stap uit de onveilige meeting en maak als beheerder een nieuwe meeting aan die beveiligd is met een sterk wachtwoord. Communiceer dit wachtwoord per telefoon aan de andere deelnemers.
- Onderzoek of het in uw videodienst mogelijk is om gebruikers actief te verwijderen uit het gesprek.

In sommige videotools heeft de beheerder de mogelijkheid om andere gebruikers te verwijderen. Dit kan dus erg behulpzaam zijn.

Negatieve mediaberichtgeving van uw aanbieder op het gebied van privacy en/ of informatiebeveiliging

Het komt vaak voor dat er op nieuwspagina's en sociale mediaberichten worden gepubliceerd die stellen dat een bepaalde aanbieder onveilig is. Wat doet u wanneer het een aanbieder betreft die u gebruikt?

- Onderzoek of de negatieve berichtgeving impact heeft op uw organisatie.
  Het is namelijk niet altijd zo dat bijvoorbeeld alle diensten van de aanbieder onveilig zijn.
- Analyseer de risico's van het gebruik van de aanbieder.
  Hoewel de ene aanbieder minder sterke beveiligingsmaatregelen heeft, is het niet zo dat u deze niet kunt gebruiken. Het is belangrijk om te bedenken wat u precies nodig heeft en welke beveiliging daarvoor nodig is. Zoom is onlangs veel in het nieuws geweest omdat het onveilig is. Echter is er een verschil of u Zoom wilt gebruiken voor een sales gesprek of bijvoorbeeld een persoonlijk coaching gesprek.
- Houdt updates in de gaten
  Mede door de negatieve media-aandacht passen aanbieders snel beveiligingsmaatregelen aan. Zoom heeft ook nadat bekend werd gemaakt dat het platform onveilig is, snel enkele aanpassingen gemaakt in hun beveiliging.

2. Communiceer

Het is belangrijk om naast de wettelijke verplichting (zoals het melden van een datalek bij de AP), ook uw medewerkers en externe contacten op de hoogte te houden.

Er is een datalek bij u of uw aanbieder

- Licht betrokkenen in als dit noodzakelijk is.
  In sommige gevallen is het nodig om de betrokkene(n) te informeren, als er een risico voor hen is naar aanleiding van het datalek.
- Is er sprake van imagoschade?
  De Universiteit van Maastricht was slachtoffer van een ransomware aanval waarbij veel bestanden werden vergrendeld. De Universiteit heeft toen openlijk moeten toegeven dat ze geld hebben overgemaakt om geen verdere (imago)schade te leiden door een maand dicht te moeten.
- Zijn er nog sectorspecifieke instanties of autoriteiten die ingelicht moeten worden over het incident?
  Zoals Autoriteit Consument en Markt of de Autoriteit Financiële markten.

Uw videomeeting blijkt onveilig te zijn

- Communiceer naar betrokkenen hoe u de meeting voort wilt zetten.
  Nadat u de meeting heeft gesloten kunt u via een alternatieve communicatie manier (e-mail/telefoon) afspreken hoe u een volgende meeting wilt inplannen, of hoe u de bestaande meeting wilt voortzetten (door middel van een wachtwoord etc.)
- Zijn er mogelijk individuen geraakt door de onveilige situatie?
  Recentelijk werd er in een openbare Zoommeeting van de gemeenteraad van West Betuwe verstoort door een onbekende die racistische taal uitsloeg en pornobeelden toonde. De beelden van deze openbare meeting stonden niet veel later op verschillende mediakanalen waardoor ook andere deelnemers herkenbaar in beeld kwamen. Neem in zo'n geval persoonlijk contact op met de betrokkenen.

U gebruikt een systeem dat negatief in de media is gekomen

- Als uw thuiswerksysteem onveilig blijkt te zijn, zorg er dan direct voor dat medewerkers hiervan op de hoogte worden gebracht. Wanneer het gaat om een systeem waarbij van afstand ingelogd kan worden op een werkserver (zoals Citrix), zorg er dan voor dat er tot nader order geen gebruik van wordt gemaakt.
- Als een thuiswerktool (zoals Zoom) onveilig blijkt te zijn, zorg er ook dan voor dat medewerkers geen gebruik meer maken van deze tool of weten onder welke voorwaarden zij hier wel gebruik van kunnen maken. Overstappen naar een andere aanbieder? In dit overzicht staat een vergelijking van dertien populaire videoconferencing-tools.

3. Voorkom herhaling

Voorkomen is beter dan genezen, ook met thuiswerken. Ten tijde van de coronacrisis heeft een mogelijk datalek verdergaande gevolgen dan hiervoor. Vanuit de overheid ligt immers het advies om zo veel mogelijk thuis te werken.

- Informeer werknemers over de gevaren die gepaard gaan met thuiswerken.
  Het is bekend dat criminelen gebruik maken van actuele situaties en hierop inspelen. Als u slachtoffer wordt van een datalek is het belangrijk dat werknemers worden geïnformeerd over het incident zodat dit niet een tweede keer voorkomt.
- Creëer bewustwording.
  Uiteindelijk is het belangrijk dat werknemers zich bewust worden van alle mogelijke gevaren. Hieronder vallen ook phishingmails, verkeerd verzonden e-mails, etcetera. Wanneer een werknemer een dergelijke e-mail ontvangt moet dit altijd binnen een organisatie gemeld worden zodat er intern stappen kunnen worden ondernomen.

Dit verdiepingsartikel is geschreven door Geoffrey van den Bergh, Cranium Nederland, e-mail: nl-info@cranium.eu, www.cranium.eu/nl/

Dit is een artikel van de redactie van FA Rendement

FA Rendement is dé informatiebron voor administrateurs, boekhouders, controllers en andere financiële professionals. Wat is er veranderd op het gebied van financieel-administratieve wet- en regelgeving, en hoe kunt u als specialist deze informatie direct in uw dagelijkse werk toepassen? Daarnaast moet u op de hoogte zijn van onder meer de fiscaliteit, automatisering, de loon- en salarisadministratie, sociale voorzieningen, debiteurenbeheer en inkoop.

De onafhankelijke en ervaren redactie van FA Rendement zit bovenop het nieuws en vertelt u als eerste wat de ontwikkelingen zijn. Altijd in heldere taal en met een praktische insteek, zodat u de informatie direct kunt vertalen naar uw eigen werksituatie. FA Rendement is daarnaast multimediaal. De voor uw vakgebied relevante informatie verschijnt:

- ✓ dagelijks op het digitale platform Rendement Online, waar u onder meer het laatste nieuws, checklists, rekentools, maatwerkbrieven en verdiepingsartikelen tot uw beschikking heeft;
- ✓ wekelijks gebundeld in een e-mailnieuwsbrief;
- ✓ maandelijks in het vakblad FA Rendement, boordevol nieuws en achtergrondartikelen, digitaal en op de mat;
- ✓ tweemaandelijks in een handzaam themadossier: een pocketboekje dat iedere editie een complex onderwerp uitdiept.