Risico inventarisatie en -evaluatie Veilig digitaal thuiswerken

Januari 2025

Inhoudsopgave

Voorwoord

Nu thuiswerken steeds vaker de norm is, wordt digitale veiligheid belangrijker dan ooit. Hoewel dit flexibiliteit en efficiëntie biedt, brengt het ook uitdagingen met zich mee op het gebied van digitale weerbaarheid. Het waarborgen van een veilige thuiswerkplek is essentieel om bedrijfsgegevens te beschermen en cyberdreigingen te minimaliseren. In deze blog bespreken we de belangrijkste aandachtspunten en maatregelen voor het creëren van een veilige thuiswerkplek, met inzichten van Bol Adviseurs en andere betrouwbare bronnen.

Als werkgever heb je de wettelijke verplichting om een veilige en gezonde werkplek te bieden, ook wanneer medewerkers vanuit huis werken. Dit omvat zowel de fysieke als digitale aspecten van de thuiswerkplek. Het is belangrijk om de risico's van thuiswerken te inventariseren en vast te leggen in een Risico-Inventarisatie en -Evaluatie (RI&E). Dit document biedt je houvast in de strijd tegen cyberdreigingen.

Mocht je naar aanleiding van deze publicatie vragen hebben over de gevolgen in jouw specifieke situatie? Neem dan contact met ons op. We helpen je graag een stapje vooruit.

Roy Verbroekken
Partner Bol Adviseur
Senior Adviseur Digitale Weerbaarheid

Veilig digitaal thuiswerken

Thuiswerken, of werken vanaf elke locatie, is tegenwoordig een vast onderdeel van ons leven. Dankzij technologische innovaties, zoals cloudopslag, VOIP en videoconferenties, is dit eenvoudiger dan ooit. Maar wist je dat er ook risico's verbonden zijn aan werken buiten kantoor?

Voor ondernemers is het daarom cruciaal om duidelijke afspraken te maken met medewerkers over veilig digitaal thuiswerken. Zo bescherm je niet alleen je bedrijf, maar ook de gegevens van je klanten.

Wat zijn de risico's van thuiswerken?

Bedrijven besteden vaak veel aandacht aan digitale beveiliging op kantoor. Denk hierbij aan het installeren van antivirussoftware, firewalls en het gebruik van een beveiligd wifi-netwerk. Maar zodra medewerkers buiten kantoor werken, kunnen nieuwe uitdagingen ontstaan:

- Gebruik van privé-apparatuur: Werknemers gebruiken soms hun eigen computer, die mogelijk gedeeld wordt met andere gezinsleden. Dit kan leiden tot veiligheidsrisico's als de computer niet goed beveiligd is.
- Onveilige thuisnetwerken: Thuisrouters zijn vaak minder goed beveiligd dan zakelijke netwerken. Dit maakt het makkelijker voor hackers om in te breken.

Het gevolg? De kans dat gevoelige bedrijfsgegevens in verkeerde handen vallen wordt groter.

Veilig thuiswerken: Afspraken en technieken

Afspraken voor veilig werken

- Apparatengebruik: Sta privé-apparaten toe onder strikte richtlijnen, zoals up-to-date software en bescherming tegen malware.
- Wachtwoorden: Gebruik unieke wachtwoorden en wachtwoordmanagers.
- Thuisnetwerk: Adviseer een sterk wifi-wachtwoord, router-updates en een VPN.
- Schermbeveiliging: Laat medewerkers schermen vergrendelen en uitloggen bij afwezigheid.

Veilige techniek voor thuiswerken

- VPN-verbinding: Versleutelt gegevens en beschermt tegen onderschepping.
- Veilige webapplicaties: Gebruik goed beveiligde tools met versleuteling.
- Twee-factor-authenticatie: Voeg een extra beveiligingslaag toe via een app of sms.
- Remote Desktop: Stel veilige instellingen in en update systemen regelmatig.

Doe de risico-inventarisatie!

Zoals eerder aangegeven, brengt thuiswerken bepaalde beveiligingsrisico's met zich mee. Daarom hebben wij risico-inventarisatietabellen opgesteld, zodat je meer inzicht krijgt over de bijhorende maatregelen en beoordelingen die relevant voor jou zijn. Zie hieronder de tabellen.

1. Identificatie van risico’s

Nr	Risico	Beschrijving	Impact (Hoog/ Midden/ Laag)	Waarschijn-lijkheid (Hoog/Midden /Laag)	Prioriteit (Hoog/ Midden/ Laag)
1	Onbeveiligd thuisnetwerk	Medewerkers gebruiken een niet-beveiligd, wifi-netwerk, waardoor derden toegang kunnen krijgen tot data.	Hoog	Midden	Hoog
2	Gebruik van privé-apparatuur	Apparaten zonder antivirus of updates worden gebruikt voor toegang tot bedrijfsdata.	Hoog	Hoog	Hoog
3	Onvoldoende wachtwoord-beheer	Zwakke of hergebruikte wachtwoorden vergroten de kans op ongeoorloofde toegang	Hoog	Hoog	Hoog
4	Geen gebruik van tweefactor-authenticatie	Applicaties en data zijn niet extra beveiligd met tweefactor-authenticatie	Hoog	Midden	Hoog
5	Onveilige bestandsdeling	Gebruik van onbeveiligde platforms voor het delen van gevoelige bestanden	Midden	Hoog	Midden

Nr.	Risico	Beschrijving	Impact (Hoog/ Midden/ Laag)	Waarschijn-lijkheid (Hoog/Midden /Laag)	Prioriteit (Hoog/ Midden/ Laag)
6	Remote Desktop zonder beveiliging	Onveilige configuraties van Remote Desktop Protocol (RDP) vergroten risico op ransomware-aanvallen	Hoog	Midden	Hoog

2. Beoordeling van maatregelen

Nr	Maatregel	Toelichting	Status (Niet gestart/In uitvoering /Gereed)	Deadline	Verant-woordelijk-heid
1	Beveiliging thuisnetwerken verbeteren	Richtlijnen geven over het instellen van een sterk wifi-wachtwoord en versleutelde verbindingen (bijv. WPA3).	[.....]	[Datum]	[Naam]
2	Bedrijfs-apparatuur	Medewerkers voorzien van laptops met vooraf geïnstalleerde beveiligingssoftware.	[.....]	[Datum]	[Naam]
3	Wachtwoord-Beheer verbeteren	Implementeren van een wachtwoordmanager en training over het gebruik van sterke wachtwoorden.	[.....]	[Datum]	[Naam]
4	Tweefactor-authenticatie verplichten	Invoeren van tweefactorauthenticatie voor alle zakelijke applicaties en systemen.	[.....]	[Datum]	[Naam]
5	Beveiligde platformen aanwijzen	Alleen goedgekeurde tools zoals SharePoint of OneDrive toestaan voor het delen van bedrijfsbestanden.	[.....]	[Datum]	[Naam]
6	Remote Desktop zonder beveiligen	RDP configureren met sterke versleuteling en IP-whitelisting om ongeautoriseerde toegang te voorkomen.	[.....]	[Datum]	[Naam]

3. Planning en monitoring

Activiteit	Frequentie	Verantwoor-delijke	Status (Niet gestart/In uitvoering/ Gereed)	Opmerkingen
Evaluatie van de thuiswerkbeveiliging	Elke 6 maanden	IT-afdeling	[.....]	Eerste evaluatie gepland in: [maand].
Medewerkerstraining over cyberveiligheid	Jaarlijks	HR en IT	[.....]	Trainingsmateriaal in ontwikkeling
Updates beveiligingsrichtlijnen	Elk kwartaal	IT-beheerder	[.....]	Regelmatige controle van VPN-instellingen

4. Samenvatting en acties

- Totaal aantal geïdentificeerde risico's: [Aantal]
- Hoogste prioriteit: [Opsomming van de risico's met hoge prioriteit]
- Acties gepland: [Samenvatting van geplande maatregelen]
- Evaluatiedatum: [Datum volgende evaluatie]

Wil jij jouw digitale weerbaarheid vergroten?

Om de digitale weerbaarheid van je bedrijf op topniveau te brengen, bieden we een uniek programma. Daarbij begeleiden we je niet alleen bij technische oplossingen, maar helpen we ook om het bewustzijn van medewerkers te verhogen en om informatiebeveiliging te integreren in de dagelijkse manier van werken.

Het digitale weerbaarheids-programma begint altijd met onze risicoanalyse of Maturity Scan. Deze nulmeting brengt het huidige weerbaarheidsniveau in kaart. Na een heldere, multidisciplinaire analyse weet je of jouw onderneming in staat is om risico's preventief te beheersen, gevaar tijdig te ontdekken en hoe te handelen als het mis gaat.

We bieden concrete oplossingen om jouw digitale weerbaarheid te verbeteren. Hierbij heb je de keuze uit meer dan 20 diensten, gericht op preventieve, detectieve en corrigerende maatregelen. Vanuit een regisseursrol helpen we je met het plannen en prioriteren van de acties en bij de uitvoering ervan – soms door externe specialisten.

Bekijk het onze website of neem contact op met één van de specialisten voor meer informatie.

Roy Verbroekken
Partner Bol Adviseur
Senior Adviseur Digitale Weerbaarheid
088 12 11 321
r.verbroekken@boladviseurs.nl

Thijs Peeters
EDP-auditor
Senior Adviseur Digitale Weerbaarheid
088 12 11 351
t.peeters@boladviseurs.nl

Afsluiting

Heb je naar aanleiding van deze publicatie vragen of wil je weten hoe de je de informatie uit deze publicatie kunt interpreteren in jouw specifieke situatie? Neem dan contact met ons op. Onze adviseurs staan voor je klaar!

Je kunt alle vragen naar ons mailen via info@boladviseurs.nl of telefonisch contact met ons opnemen. Verder nodigen we je van harte uit om onze website www.boladviseurs.nl regelmatig te bezoeken. Hier vind je updates over wijzigingen in wet- en regelgeving, interessante blogs, actuele nieuwsberichten en concrete tips voor ondernemers. Zo blijf je altijd op de hoogte!

Zo dichtbij is Bol!

Bol Adviseurs heeft 5 vestigingen. Daarmee bevinden we ons dichtbij onze klanten. We zijn gevestigd in, Boxmeer, Nijmegen (Wijchen), Venray, Venlo en Veghel.

Bol Adviseurs
Postbus 142
5830 AC Boxmeer
T +31 88 1211 300
E info@boladviseurs.nl
www.boladviseurs.nl