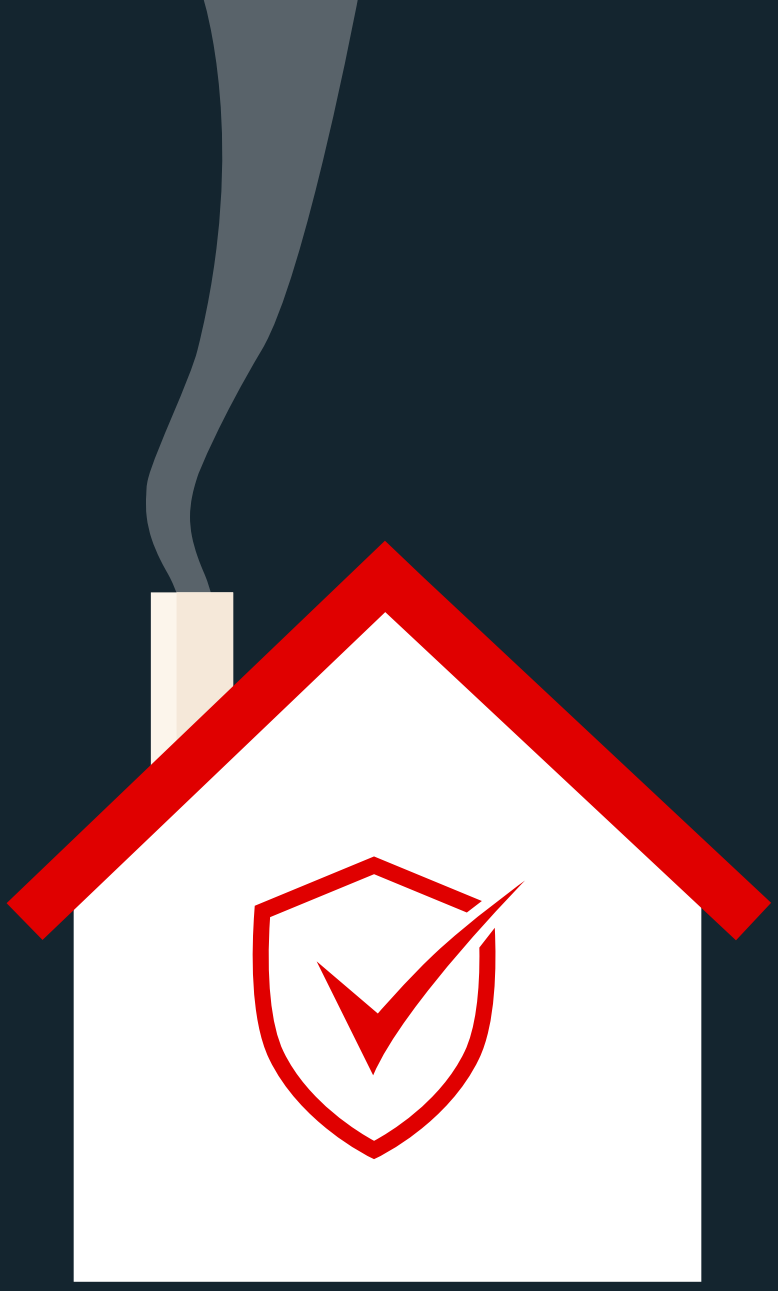

Security

Snelle checklist voor veilig thuiswerken

claranet

Veilig thuiswerken

Onbeveiligde wifi-netwerken, veilige devices gebruiken om te werken, thuisnetwerken, phishing-zwendel gericht op thuiswerkers. De inkt van het nieuwe thuiswerkbeleid van organisaties is wellicht nog aan het drogen terwijl we langzaam wennen aan onze nieuwe werkomgeving. Veilig werken op afstand is hier een essentieel onderdeel van en de onderstaande checklist bevat enkele belangrijke aandachtspunten. Zoals altijd, als je het niet zeker weet, vraag het ons. Want er kunnen specifieke aanbevelingen zijn met betrekking tot hoe jouw organisatie werkt en waar welke collega's die werken toegang toe nodig hebben.

Hier hebben we een checkklist voor je.

Toegang op afstand	Beslis hoe de toegang op afstand zal worden verleend, b.v. VPN (IPSec of SSL-VPN), directe toegang, portalgebaseerd (SSL-VPN) of externe beveiligde desktop-toegang. Zorg ervoor dat de ondersteunende infrastructuur geschikt is om aan de vraag te voldoen (d.w.z. internetbandbreedte, licenties, serverresources, etc).
Toegestane devices	Idealiter zou toegang tot bedrijfsbronnen alleen toegankelijk moeten zijn via vertrouwde devices. Meestal worden deze apparaten geleverd door de eigen IT-afdeling en daarom moet de beveiliging van deze apparaten bekend en vertrouwd zijn. Dit kan problematisch zijn tijdens de huidige COVID-19-crisis, dus overweeg oplossingen die kunnen worden gecontroleerd met additionele, beveiligde toegang (bijv. Citrix, Terminal Services, WorkSmart365) waar minder vertrouwde apparaten kunnen worden gebruikt.
Authenticatie	Sterke authenticatie is essentieel voor een thuiswerkoplossing. Devices zijn niet beschermd tegen het niet-vertrouwde openbare internet met behulp van firewalls en andere beveiligingsapparaten, dus het is belangrijk dat de authenticatiemechanismen en oplossingen voor externe toegang robuust genoeg zijn om te beschermen tegen pogingen tot inbraak via bijvoorbeeld 'brute force' wachtwoordaanvallen. Multi-factor authentication moet worden ingezet als verdere verdediging tegen inbraakpogingen en om verdere zekerheid te bieden dat de gebruiker die probeert in te loggen daadwerkelijk de beoogde gebruiker is.
Autorisatie	Gebruikers mogen alleen toegang krijgen tot systemen en gegevens waartoe zij zakelijk toegang nodig hebben, zodat die gebruiker zijn taak kan uitoefenen. Een correct geconfigureerde en veilige oplossing voor thuiswerken moet de gebruiker dezelfde toegang bieden als via het interne netwerk.

claranet

Gebruikerstoegangsbeheer	Het is belangrijk dat de oplossing voor externe toegang voldoende schaalbaarheid en gelaagdheid kan bieden om de toegang van gebruikers tot gegevens en systemen te helpen beperken. Onjuist geconfigureerde thuiswerkoplossingen kunnen bredere toegang bieden aan externe gebruikers, hetzij door verkeerde configuratie of door een gebrek aan functionaliteit binnen de oplossing.
Apparaatversleuteling	Waar toegestane apparaten in contact kunnen komen met vertrouwelijke gegevens moeten deze apparaten krachtige schijfversleuteling gebruiken om deze gegevens te beschermen. Dit kan voor eigen devices (of BYOD) problematisch zijn. Dit probleem kan worden opgelost wanneer de juiste oplossingen worden geïmplementeerd waarbij er gezorgd wordt dat gegevens niet wordt opgeslagen op het device zelf.
Opslag van gegevens	Organisaties hebben de zorgplicht om bedrijfsgegevens, creditcardgegevens en klantgegevens, met name vertrouwelijke, te beschermen. De meest effectieve manier om dit te bereiken is door de toegang en opslaglocaties van de gegevens te beperken. Door opslaglocaties te beperken, kunnen organisaties beveiligingsmechanismen en toegangscontroletechnieken inzetten om gegevens te beschermen tegen ongeoorloofde toegang, wijziging en verwijdering. Naarmate organisaties beginnen met het uitbreiden van opslaglocaties, wordt het veel moeilijker om de toegang en de beveiliging van de gegevens te beheren. Als er geen technologieën en mechanismen worden geïmplementeerd om te voorkomen dat gegevens worden opgeslagen op devices die worden gebruikt voor externe toegang, wordt het buitengewoon moeilijk om adequate beveiligingscontroles te bieden. Dit zal problemen veroorzaken met betrekking tot AVG-gerelateerde zaken, aangezien organisaties geen volledige zichtbaarheid hebben waar gegevens zich bevinden.
Goedgekeurde communicatieplatforms en tooling	Bij werken op afstand zouden medewerkers hun eigen applicaties en tools kunnen gebruiken in plaats van die van hun organisatie. Bepaal een bedrijfsstrategie voor goedgekeurde software die door werknemers MOET worden gebruikt en maak deze gebruiksvriendelijk. Het gebruik van tools zoals DropBox kan betekenen dat bedrijfsgegevens of gevoelige informatie worden opgeslagen op plaatsen zonder bewaking en met lagere beveiligingscontroles. Hierdoor kunnen dataprivacy en compliance in gevaar worden gebracht en dat kan in sommige gevallen aanzienlijke kosten veroorzaken.
Malware en Endpoint Security	Malware neemt toe en aanvallers manipuleren al angst die verband houdt met COVID-19 om de thuiswerkers te misleiden. Beveilingstools op het device zijn essentieel in het bestrijden van malware-aanvallen. Gebruik waar mogelijk malwarebescherming van de volgende generatie aangezien deze meer mogelijkheden hebben om nieuwe en niet-geclassificeerde aanvallen te detecteren die traditionele antivirusprogramma's missen.

Patching-beleid	Devices moeten worden geconfigureerd om automatisch updates van de softwareleveranciers uit te voeren. Centraal beheerde tools voor patchbeheer (uitgezonderd cloudservices zoals Microsoft InTune) zijn goed te gebruiken, maar overweeg hoe vaak de gebruikers verbinding maken met het netwerk om updates te ontvangen. Als het niet vaak genoeg is, kunnen devices ongepatcht blijven en kwetsbaar worden voor een inbreuk.
Sessie vergrendelen	Zorg ervoor dat externe sessie worden vergrendeld na een acceptabele periode van inactiviteit (misschien 15 minuten). Om toegang te krijgen, moet de gebruiker zich opnieuw verifiëren.
Toegang toestaan vanaf eigen onbeheerde apparaten (BYOD)	Als gebruikers of derden verbinding met het netwerk moeten maken, maar het device niet wordt beheerd door de IT-afdeling, overweeg dan om virtuele desktopomgevingen te implementeren voor connectiviteit op afstand. Het werkt net als een volledige computer met een besturingssysteem en toepassingssoftware, maar biedt zakelijke controle voor updates, beveiligingsconfiguratie en gegevensbeveiliging. Claranet biedt hiervoor WorkSmart365. Bovendien worden veel oudere Windows-besturingssystemen nu niet meer ondersteund, waardoor ze kwetsbaar kunnen worden. Zorg ervoor dat er een minimale OS-versie wordt gebruikt. XP en Windows 7 mogen niet langer worden toegestaan.
Gebruik altijd back-ups	Wat zou er gebeuren als je jouw gegevens kwijtraakt? De oorzaak kan variëren van hardware storingen tot vastlopen van applicaties en diefstal van een device. Gebruikers van Office 365 of andere cloudgebaseerde applicaties moeten altijd bedrijfsgegevens opslaan in de cloud. Back-up én Disaster Recovery kunnen in de cloud geregeld worden met Veeam back-up voor Office 365.
Beveiligingsbewaking	Logboeken vastleggen en analyseren op kwaadaardige activiteiten zoals malware of ransomware-aanvallen of ongeautoriseerde inlogpogingen is van cruciaal belang in de strijd om een datalek te voorkomen of in te perken. Zorg ervoor dat logboeken zijn gecorreleerd, dat waarschuwingen snel worden opgemerkt en dat regelmatige activiteitenbeoordelingen plaatsvinden.

Filteren van e-mail en webcontent	Bij contentfilteren wordt een programma gebruikt om de toegang tot webpagina's of e-mails met inhoud die als verwerpelijk worden beschouwd, af te schermen en/of uit te sluiten. Contentfiltering wordt zowel door bedrijven gebruikt als onderdeel van hun firewalls als door eigenaren van thuiscomputers. Het werkt door inhoudspatronen op te geven, zoals tekstreeksen of objecten in afbeeldingen die, indien ze overeenkomen, aangeven dat ongewenste inhoud moet worden afgeschermd. Een contentfilter blokkeert vervolgens de toegang tot deze inhoud voordat een gebruiker op de link kan klikken.
IT-ondersteuning	Gebruikers hebben ondersteuning nodig, tokens gaan mogelijk verloren en verbindingen kunnen instabiel zijn. Hoe zorg je ervoor dat jouw medewerkers de ondersteuning krijgen die ze nodig hebben om productief te blijven? • IT-ondersteuning - Alles van vergrendelde accounts tot defecte hardware. • Problemen oplossen - Gebruik externe sessies en realtime monitoring om te helpen • Desktops en apparaten inrichten - Hoeveel tijd is er nodig om nieuw personeel aan boord te krijgen? Gebruik screenhots om de implementatie te versnellen. Zorg ervoor dat jouw organisatie een robuust mechanisme heeft om de identiteit van een eindgebruiker te valideren VOORDAT je een wachtwoord opnieuw instelt of andere accountwijzigingen doorvoert.
Systeembeheer	Zorg voor de beschikbaarheid van het systeem voor externe toegang door een beleid en programma voor bewaking en onderhoud te ontwikkelen om systemen gezond, gepatcht en operationeel te houden.
Bewustwording van gebruikers	Thuiswerkers moeten beschikken over een basisbewustzijnsniveau om te voorkomen dat ze het slachtoffer worden van een phishing-aanval, om de risico's van gedeelde WIFI te begrijpen en om ervoor te zorgen dat thuisnetwerken correct zijn geconfigureerd. Het is een goed idee om een checklist en regelmatige herinneringen aan thuiswerkers te sturen over hoe ze nu deel uitmaken van de verdediging van de organisatie en dat er eenvoudige acties kunnen worden ondernomen om het risico te beperken.

www.claranet.nl
040 - 239 3300