logitech

CYBERBEVEILIGING VERBETEREN IN EEN UITBREIDEND RISICOLANDSCHAP

Hoe beveiligde verbindingen tussen draadloze randapparatuur kunnen helpen de gevolgen van cyberincidenten te beperken en werknemers te ondersteunen op de hybride werkplek.

De nieuwe logica van werk

Inhoudsopgave

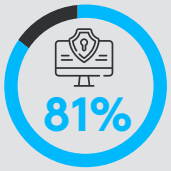
De nieuwe logica van werk: risico en realiteit

Sinds de pandemie zijn we in korte tijd op een heel andere manier gaan werken. Bedrijven haastten zich in eerste instantie om werken op afstand makkelijker te maken. Werknemers zijn een hybride omgeving niet alleen gaan waarderen, maar er ook beter in gaan werken. Tegenwoordig omarmen veel organisaties het hybride werken. Door deze verschuiving naar een dynamischere manier van werken, hebben IT-teams wereldwijd te maken gekregen met nieuwe aandachtspunten op het gebied van beveiliging. Gebruikers werken tegenwoordig waar het hun uitkomt, niet per se binnen de veilige grenzen van de firewall van het bedrijf.

De "Nieuwe logica van werk" heeft ervoor gezorgd dat de traditionele desktopcomputer niet langer optimale productiviteit biedt. Laptops hebben een centrale plek ingenomen in het werkende leven van veel mensen. Dankzij laptops kunnen werknemers productief zijn waar ze zich ook bevinden, onderweg, in een koffiehuis of thuis. De "Nieuwe logica van werk" heeft ook nieuwe bedreigingen met zich meegebracht en deze bedreigingen vormen dan ook een belangrijke bron van zorg voor It-teams. Het heeft ertoe geleid dat zakelijke apparaten en netwerken worden blootgesteld aan nieuwe risico's.

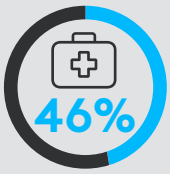
Hedendaagse risico's voor bedrijven

Het risico van een cyberincident neemt al enige tijd toe, ongeacht of u een particulier bedrijf, overheidsbedrijf, onderwijsinstelling of privépersoon bent.



Tijdens de pandemie **had 81% van de organisaties wereldwijd te maken met toegenomen cyberbeveiligingsgerelateerde activiteit**, wat bij 79% leidde tot downtime vanwege een cyberincident tijdens een drukke periode[1].

Volgens ENISA (Agentschap van de Europese Unie voor cyberbeveiliging) was er in 2020 een verdubbeling van het aantal cyberincidenten waarbij "kritieke sectoren" het doelwit waren, naast een **toename van 46% van incidenten gericht op ziekenhuizen en zorgnetwerken**[2].



Ook de kosten van een inbreuk zijn veel groter geworden. Strengere wetgeving op het gebied van gegevensbescherming, zoals de AVG in Europa, leidt ertoe dat niet alleen de reputatie, de financiële positie en de bedrijfsvoering van organisaties onder een cyberincident te lijden hebben, maar dat organisaties ook een fikse boete van tot €20 miljoen of (als dit bedrag hoger is) 4% van de wereldwijde omzet kunnen verwachten.

Aangezien de **kosten van een inbreuk gemiddeld rond de €4 miljoen liggen**, is cyberbeveiliging een onderwerp dat organisaties in alle sectoren bezighoudt. Ook moet iedere werknemer ermee bekend zijn, vooral aangezien **95% van de problemen met cyberbeveiliging het gevolg zijn van een menselijke fout in enige vorm**[3].

Cyberaanvallen worden in de meeste gevallen uitgevoerd op de zwakke plekken van doelwitten. Dit kan gaan om een foutieve coderegel op een website, een onoplettende of kwaadwillende werknemer, malware in een e-mailbijlage, een gestolen apparaat of verouderde software en hardware.

Deze risico's worden verhoogd als de werknemers niet of onvoldoende van cyberbeveiliging weten. Door een stap verder te gaan dan standaardmaatregelen voor cyberbeveiliging kunnen bedrijven de toezichthouders, hun verzekeraars en vooral hun klanten laten zien dat ze al het mogelijke hebben ondernomen om hun beveiliging op orde te houden.

In dit whitepaper bekijken we een voorbeeld van één manier waarop bedrijven, organisaties en instellingen van iedere omvang hun beveiliging kunnen verbeteren door draadloze toetsenborden en muizen te beveiligen. Hierbij maakt het niet uit of de medewerkers op kantoor, thuis of onderweg aan het werk zijn.

Een zwakke plek in de beveiliging die bedrijven vaak over het hoofd zien

Met de “Nieuwe logica van werk” hebben IT-organisaties uiteenlopende maatregelen en beleidspunten geïmplementeerd om werknemers die op afstand werken te beschermen.

Het gaat hierbij om VPN’s, verbeterde beveiligingssoftware voor eindpunten, beheersystemen voor mobiele apparaten, multifactorauthenticatie en meer. Maar zelfs als deze beschermingsmaatregelen in orde zijn, blijft er nog één kwetsbare bron van waardevolle data voor hackers over, en dat is de informatie die tussen draadloze randapparatuur en de computer zelf wordt verzonden.

Hoe kunt u randapparatuur beveiligen en uw bedrijf beter beschermen?

Om te helpen voorkomen dat inbreuk wordt gemaakt op draadloze muizen en toetsenborden, moeten IT-teams ervoor zorgen dat de verbindingen met deze apparaten zo veilig mogelijk zijn. Voor bedrijven, met name kleine en middelgrote, met beperkte beveiligingsmiddelen zijn deze maatregelen cruciaal om onbevoegde toegang tot gegevens en systemen te voorkomen.

De eerste stap is ervoor zorgen dat de firmware van alle apparaten is bijgewerkt en dat de verbindingen die met de apparaten tot stand worden gebracht versleuteld zijn.

Voor apparaten met *Bluetooth*® moet de verbinding gebruikmaken van Security Mode 1, Level 4 (Secure Connections Only-modus), die voldoet aan FIPS (Federal Information Processing Standards). Gaat het om apparaten die verbinding maken via een USB-dongle, zoek dan een anti-terugdraaifunctie voor device firmware upgrades (DFU’s) op basis van beveiliging.

Hiermee kunt u voorkomen dat kritieke beveiligingspatches per ongeluk worden verwijderd, terwijl terugdraaien nog wel mogelijk blijft voor updates die geen verband houden met beveiliging.

Hoe veilig is uw randapparatuur?

- Werkt u de firmware van apparaten regelmatig bij?
- Maken draadloze toetsenborden en muizen gebruik van een Secure Connections Only-modus?
- Kunt u voorkomen dat apparaten die met een USB-dongle verbonden zijn worden teruggedraaid naar eerdere firmwareversies?

Logi Bolt: een veilige oplossing

Naarmate de beveiligingsrisico's in een hybride wereld zijn toegenomen, zijn bedrijven anders gaan denken over draadloze computerrandapparatuur. Tegenwoordig richten organisaties zich met betrekking tot randapparatuur voornamelijk op het volgende:

- **Beveiliging**
- **Goede werking in zwaar belaste omgevingen**
- **Platformoverschrijdende compatibiliteit**

Daarom heeft Logitech een eigen protocol ontwikkeld met de naam Logi Bolt, op basis van *Bluetooth*® Low Energy (BLE), waarbij beveiligingsfuncties worden ingezet om man-in-the-middle-aanvallen af te slaan en afluisteren en code-injectie te voorkomen.
Logi Bolt-technologie is volledig versleuteld en FIPS-compliant. Dit zorgt ervoor dat een draadloos Logi Bolt-product en de Logi Bolt USB-ontvanger alleen met elkaar kunnen communiceren.

Logitech heeft als doel om de beveiliging van bedrijven te verbeteren en een betrouwbaar signaal te verschaffen met Logi Bolt. Zelfs in omgevingen die zwaar worden belast met draadloos verkeer. Logi Bolt is compatibel met alle grote besturingssystemen en platforms. Hierdoor is het gemakkelijk te installeren en te beheren, ook voor kleine IT-afdelingen.

Veilige verbinding

Logi Bolt zorgt voor communicatie tussen draadloze muizen en toetsenborden. De koppeling met de USB-ontvanger is altijd versleuteld, door middel van Authenticated Low Energy Secure Connections (LESC).

Beschermde koppeling

Logi Bolt USB-ontvangers schakelen de Secure Connection Only-modus in, waardoor bij het koppelen de twee apparaten moeten worden geverifieerd en de koppeling moet worden versleuteld.

Eenvoudig, veilig beheer

Logi Bolt is voorzien van beveiligingsmaatregelen in de vorm van zelfbediening, maar wel nog met een centraal overzicht. Zo verschijnt er een melding als er een koppelverzoek voor een nieuw apparaat wordt ingediend.

Lever niet in op keuze, comfort of productiviteit

Tegenwoordig wordt er voornamelijk op laptops gewerkt, vooral als mensen op afstand werken. Nu zijn laptops prima voor mobiliteit, maar de compacte toetsenborden en trackpads zijn niet ideaal voor de gezondheid of voor productief werk gedurende langere perioden.

Draadloze muizen en toetsenborden vormen een flexibele oplossing die werknemers de vrijheid geeft om hun invoerapparaten zo neer te zetten dat ze gemakkelijk te gebruiken zijn en niet in de weg staan.

Met Logitech for Business-oplossingen en Logi Bolt kunnen werknemers en hun organisaties enerzijds profiteren van veilige verbindingen en anderzijds van een keuze aan randapparatuur die aan hun behoeften voldoet.

Logitech for Business-oplossingen met Logi Bolt

De MX Master Series for Business

Ongeëvenaarde precisie en prestaties gecombineerd met Logi Bolt-technologie. Ideaal voor analisten, creators, programmeurs en iedereen die zeer specifieke eisen aan workflows stelt.

MX KEYS COMBO FOR BUSINESS

De combinatie MX Keys for Business en MX Master 3S for Business met handsteun is de ultieme verbinding met muis en toetsenbord voor productiviteit.

MX KEYS FOR BUSINESS

Meer productiviteit voor programmeurs, analisten en creators die stabiliteit, precisie en vermogen nodig hebben om hun werk naar een hoger niveau te tillen.

MX MASTER 3S

De MX Master 3S for Business is onze iconische muis, nu nog beter met Quiet Click-technologie. Hierdoor is het klikgeluid maar liefst 90% zachter is. De muis werkt op ieder oppervlak – zelfs op glas – met een 8K DPI-sensor met aanpasbare gevoeligheid.

MX ANYWHERE 3 FOR BUSINESS

Ultieme wendbaarheid en professionele prestaties. Ontdek de compacte muis die is ontworpen voor mobiel werk — van het thuiskantoor tot het café en de luchthavenlounge.

MX KEYS MINI COMBO FOR BUSINESS

MX Keys Mini Combo for Business. De compacte combinatie van een hoogwaardige muis en toetsenbord voor meer ruimte op de werkplek en hogere productiviteit.

MX KEYS MINI FOR BUSINESS

De MX Keys Mini for Business is dankzij zijn geavanceerde features in een gestroomlijnd, minimalistisch ontwerp uitstekend voor gebruikers die meer werkruimte nodig hebben. Denk dan met name aan creators met een veeleisende workflow.

MX MASTER 3 FOR BUSINESS

Ongeëvenaarde precisie en prestaties voor analisten, creators, programmeurs en iedereen die zeer specifieke eisen aan workflows stelt.

De Ergo Series for Business

Muizen en toetsenborden die op wetenschappelijke wijze zijn ontworpen met oog op een natuurlijker lichaamshouding en minder spierbelasting.

ERGO K860 FOR BUSINESS

Geef gebruikers de ruimte om zich te focussen met een ergonomisch toetsenbord dat een meer ontspannen, natuurlijke typervaring waarborgt. Ontworpen voor urenlang comfortabel gebruik.

LIFT FOR BUSINESS

Lift for Business is goedgekeurd door ergonomen en heeft het juiste formaat voor iedere hand: links én rechts. Deze muis verbetert de lichaamshouding en vermindert vermoeidheid van de onderarmspieren.

ERGO M575 FOR BUSINESS

Dankzij zijn wetenschappelijk ontwikkelde ontwerp en de makkelijke duimbediening, is deze draadloze trackballmuis gemaakt om handbewegingen te verminderen. Hierdoor blijven de hand en arm ontspannen voor urenlang comfort.

De Signature Series for Business

Verbeter de productiviteit, het comfort en de algemene werknemerservaring door hen te voorzien van Logitech Signature for Business-oplossingen.

SIGNATURE MK650 COMBO FOR BUSINESS

De Signature MK650 for Business Wireless Mouse is ontworpen voor comfort en verhoogt productiviteit met 50% en werksnelheid met 30% ten opzichte van de touchpad van een laptop.

SIGNATURE M650 FOR BUSINESS

De Signature M650 for Business Wireless Mouse is ontworpen voor comfort en verhoogt productiviteit met 50% en werksnelheid met 30% ten opzichte van de touchpad van een laptop.

SIGNATURE M650 L FOR BUSINESS

Wij raden de Signature M650 aan voor kleine tot middelgrote handen en de Signature M650L voor grote handen.

Meerdere apparaten

Door Logitech for Business-oplossingen met Logi Bolt te gebruiken kunnen werknemers overal sneller en productiever werken zonder dat dit ten koste gaat van de beveiliging.

Een enkele Logi Bolt-ontvanger kan worden gekoppeld aan zes Logi Bolt-apparaten met drie actieve verbindingen. Dat is met name handig voor werknemers die verschillende apparaten gebruiken als ze op kantoor, thuis of onderweg zijn.

Als de Logi Bolt-ontvanger op de laptop is aangesloten, kunnen verschillende randapparaten met Logi Bolt veilig worden gebruikt op elke locatie.

Sterker signaal, uitgebreide compatibiliteit

Als organisaties randapparatuur kiezen, is niet alleen beveiliging een belangrijke overweging, maar ook de kwaliteit en compatibiliteit van de verbinding. Logi Bolt is ontworpen voor betrouwbare verbindingen, zelfs in draadloze omgevingen met veel interferentie van wifi-toegangspunten of omringende draadloze apparaten.

De Logi Bolt USB-ontvangers bieden een betrouwbare, drop-off-vrije verbinding tot 10 meter met in veel gevallen tot 8x lagere latentie dan andere veelgebruikte ontvangers in drukke bedrijfsomgevingen met veel ruis.

Bovendien werkt Logi Bolt met nagenoeg elk besturingssysteem en platform. Logi Bolt-apparaten zijn zelfs breder compatibel dan randapparatuur van de meest toonaangevende merken in de markt.

Meer keuze zonder compromis

Er is een Logitech for Business-oplossing naar wens voor iedere gebruiker. Of het nu gaat om een zware gebruiker met een veeleisende workflow, een gebruiker die op een eenvoudige manier productiever wil zijn of een gebruiker die meer ergonomisch comfort wenst.

Logi Bolt-technologie maakt deel uit van de assortimenten Ergo, Signature en MX van Logitech for Business-toetsenborden en -muizen. Met behulp van deze producten kunnen gebruikers op de door hen gewenste manier werken zonder in te leveren op veiligheid.

Verbeterde beveiliging voor veranderende werkomstandigheden

De “Nieuwe logica van werk” van tegenwoordig brengt steeds meer cyberrisico’s met zich mee. Daarom is het belangrijk dat bedrijven weten wat de zwakke plekken in hun organisatie zijn. Dankzij Logitech for Business-randapparatuur met Logi Bolt beschikken organisaties niet alleen over een krachtige, betrouwbare verbinding en brede compatibiliteit, maar hebben ze ook meer keus als het gaat om het beschermen van hun bedrijf en het ondersteunen van hun werknemers.

Met randapparatuur met Logi Bolt kunnen bedrijven hun beveiliging snel opschroeven waar nodig, zonder dat de gebruikers eronder te lijden hebben. Dit kan gebeuren wanneer nieuwe apparaten in gebruik worden genomen of wanneer het beveiligingsbeleid wordt aangepast. Logitech hecht er veel waarde aan dat organisaties en eindgebruikers niet alleen profiteren van betere productiviteit en bescherming, maar ook van keuzevrijheid en flexibiliteit. Logi Bolt maakt dan ook deel uit van steeds meer apparaten in het randapparatuurportfolio “for business” van Logitech.

Meer informatie over Logi Bolt en Logitech for Business-oplossingen

Neem contact op met Logitech Sales

Bronnen
1. https://www.businesswire.com/news/home/20211108005775/en/Cyber-Threats-Have-Increased-81-Since-Global-Pandemic
2. https://edition.cnn.com/2021/06/10/tech/europe-cyberattacks-ransomware-cmd-intl/index.html
3. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

© 2022 Logitech. Logitech, Logi, Logi Bolt en het Logitech-logo zijn handelsmerken of gedeponeerde handelsmerken van Logitech Europe S.A. en/of zijn dochterondernemingen in de VS en andere landen. Het *Bluetooth*®-woordmerk en de *Bluetooth*®-logo’s zijn het eigendom van Bluetooth SIG, Inc. en elk gebruik van dergelijke merken door Logitech is onder licentie.