ZORGEN VOOR DE BEVEILIGING VAN DRAADLOZE MUIZEN EN TOETSENBORDEN BIJ THUISGEBRUIK

Het handhaven van de bedrijfsbeveiliging is van cruciaal belang in de huidige wereld van steeds groter wordende cyberdreigingen. De draadloze muizen en toetsenborden die uw werknemers elke dag gebruiken, maken integraal deel uit van het totale beveiligingslandschap.

HIER ZIJN EEN PAAR PUNTEN OM TE OVERWEGEN BIJ HET BEOORDELEN VAN DE VEILIGHEID VAN DE DRAADLOZE RANDAPPARATUUR VAN UW BEDRIJF.

- ☐ **Weet welke apparaten verbonden zijn met uw endpoints.** Als uw werknemers muizen en toetsenborden gebruiken die niet van uw organisatie afkomstig zijn of als uw organisatie geen lijst heeft met apparaten die goedgekeurd zijn voor gebruik, kan er van alles gebeuren.
- ☐ **Zorg ervoor dat deze apparaten versleutelde verbindingen hebben.** Versleutelde verbindingen voorkomen dat hackers apparaten als 'wifi-sniffers' gebruiken en op afstand toetsaanslagen en muisklikken onderscheppen.
- ☐ **Update de firmware op de apparaten.** Verouderde firmware kan apparaten kwetsbaar maken voor bekende misbruikpraktijken.
- ☐ **Zorg ervoor dat *Bluetooth*®-apparaten gebruikmaken van Security Mode 1, Level 4.** Deze instelling helpt verbindingen tussen apparaten te beveiligen.
- ☐ **Voorkom dat apparaten met USB-dongles de beveiligingsfirmware kunnen terugdraaien.** Apparaten die beveiligingsgerelateerde firmware-upgrades kunnen terugdraaien, kunnen uw endpoints blootstellen aan aanvallen.
- ☐ **Informeer uw werknemers over aanvallen gericht op muizen en toetsenborden.** Naast voorlichting over de bescherming tegen malware en phishing, moet u ervoor zorgen dat uw werknemers weten dat vreemd gedrag van een muis of toetsenbord een teken kan zijn dat iemand onbevoegd de controle heeft overgenomen.

Logitech-oplossingen helpen beveiligingsfuncties te implementeren in zakelijke apparatuur in een wereld waarin overal vandaan wordt gewerkt. Ontdek vandaag nog de nieuwste Logi Bolt-apparaten voor uw werknemers.

logitech | for business