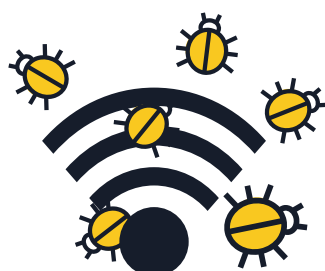
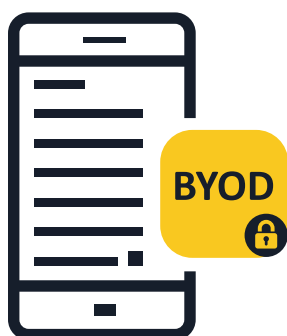


MOBIELE MALWARE

TIPS EN ADVIEZEN VOOR BEDRIJVEN



1 Informeer uw personeel over de risico's van mobiele apparaten

- Door 'mobiel werken' vervagen de grenzen tussen zakelijk en persoonlijk gebruik. Bedrijven kunnen schade oplopen als gevolg van een aanval die in eerste instantie gericht was op het mobiele apparaat van een individu. Een mobiel apparaat is een computer en moet ook beveiligd zijn.

2 Voer een bring-your-own-device-beleid (BYOD) in binnen uw bedrijf

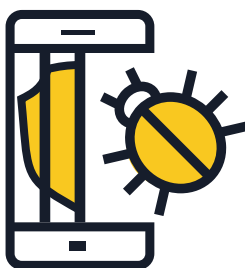
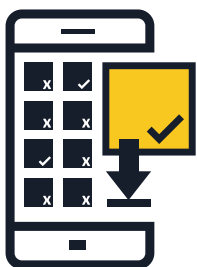
- Medewerkers die hun eigen apparaten gebruiken om toegang te krijgen tot de gegevens en systemen van hun bedrijf moeten de bedrijfsrichtlijnen volgen – ook als ze slechts hun e-mail, kalender of contactpersonen gebruiken. Selecteer de technologieën die u gebruikt om mobiele apparaten te beheren en beveiligen zorgvuldig en zorg ervoor dat uw medewerkers voorzichtig te werk gaan.

3 Zorg ervoor dat uw veiligheidsarchitectuur ook een mobiele-beveiligingsbeleid bevat

- Als een apparaat niet voldoet aan de beveiligingseisen, mag het niet gebruikt worden om verbinding te maken met het bedrijfsnetwerk of om bedrijfsgegevens te openen. Bedrijven moeten hun eigen Mobile Device Management- (MDM) of Enterprise Mobility Management-oplossingen (EMM) implementeren.
- Daarnaast is het verstandig ze ook een Mobile Threat Defence-oplossing (MTD) installeren. Dit verhoogt de zichtbaarheid en contextuele bewustwording van de risico's die apps, netwerken en besturingssystemen met zich meebrengen.

4 Let op bij het openen van bedrijfsgegevens via openbare Wi-Fi-netwerken

- De meeste openbare Wi-Fi-netwerken zijn niet beveiligd. Als een medewerker bedrijfsgegevens opent via een onbeveiligd Wi-Fi-netwerk op een vliegveld of in een café, kunnen deze gegevens ingezien worden door onbevoegde personen. Om dit te voorkomen, kunnen bedrijven een beleid voor 'effectief gebruik' implementeren.



5 Zorg ervoor dat uw besturingssystemen en apps actueel zijn

- Adviseer uw medewerkers om software-updates voor het besturingssysteem van hun mobiele apparaten te downloaden zodra deze beschikbaar zijn. Met name voor Android-systemen is het verstandig om onderzoek te doen naar het updatebeleid van mobiele providers en de fabrikanten van mobiele telefoons. Door de meest recente updates te installeren, zorgt u er niet alleen voor dat uw apparaat beter beveiligd is, maar ook dat het beter werkt.

6 Installeer alleen apps van betrouwbare bronnen

- Bedrijven moeten ervoor zorgen dat er alleen apps van officiële bronnen zijn geïnstalleerd op mobiele apparaten die verbinding maken met het bedrijfsnetwerk. Zo kunnen zij bijvoorbeeld een bedrijfs-appstore oprichten, waar eindgebruikers alleen door het bedrijf goedgekeurde apps kunnen openen, downloaden en installeren. Neem contact op met uw beveiligingsleverancier voor hulp met de installatie of het opzetten van uw eigen appstore.

7 Jailbreaking tegengaan

- Bij een jailbreak worden de veiligheidsbeperkingen van het besturingssysteem verwijderd, waardoor gebruikers volledige toegang krijgen tot het besturingssysteem en alle hieraan gekoppelde functies. Door uw mobiele apparaat te jailbreaken, kunt u verborgen beveiligingsproblemen blootleggen, waardoor u een verhoogd veiligheidsrisico loopt. Het gebruik van apparaten met root-functionaliteit moet binnen de bedrijfsomgeving verboden zijn.

8 Overweeg cloudgebaseerde opslagsystemen

- Mobiele gebruikers hebben vaak toegang nodig tot belangrijke documenten; niet alleen via hun werkcomputer, maar ook buiten het kantoor met hun eigen telefoon of tablet. Bedrijven kunnen een beveiligd, centrale opslag - en synchronisatiesysteem opzetten om op een veilige manier aan deze behoefte tegemoet te komen.

9 Motiveer uw medewerkers om een mobiele-beveiligingsapp te installeren

- Alle besturingssystemen kunnen geïnfecteerd raken met een virus. Zorg er, indien mogelijk, voor dat uw medewerkers een mobiele-beveiligingsoplossing gebruiken die malware, spyware en kwaadwillende apps opspoot en elimineert, en daarnaast beschikt over andere privacygerelateerde en antidiestalfuncties.