En av världens största IT-mässor, Mobile world congress i spanska Barcelona, lockar årligen över 100 000 besökare.

Spaning

Mobil (o)säkerhet på Mobile world

En av världens största IT-mässor, Mobile world congress, i Barcelona, lockar varje år över 100 000 besökare.

Här skriver Bogdan Botezatu, IT-säkerhetsexpert hos Bitdefender, om vad han tog med sig från mässan. Tyvärr lyste säkerhet med sin frånvaro.

TEXT **BOGDAN BOTEZATU**

Mobile world congress (MWC) samlar årligen tusentals besökare från världens alla hörn och årets event var inget undantag. Man lockade 108 000 deltagare från över 200 länder och 2 200 utställare. Under fyra dagar fylldes de nio gigantiska mässhallarna av drönare och robotar i alla dess former, virtuell verklighet, smarta appar och självklart uppkopplade bilar, motorcyklar och hushållsapparater.

FLYGANDE TEKNIK OCH nya mobiler i all ära, jag åkte huvudsakligen till MWC för att ta del av säkerhetstänket kopplat till vår senaste teknik.

Säkerheten och säkerhetsrisker som kan kopplas till våra smarta telefoner är extra intressant då de är ett kommunikationsverktyg som används på snart alla svenska företag och i många fall kopplar samman privatliv med arbetsliv.

Veckan rivstartade med att Adobe under mässans första dag publicerade rapporten ”Digital insights mobile world congress” som fått genomslag världen över. Rapporten visar att Sverige är det land med högst webbtrafik via smarta telefoner i Europa. Andelen datatrafik som går via sådana har i Sverige ökat från 25 procent 2014 till 39 procent 2016.

Samtidigt siade Gartner om att en fjärdedel av alla världens företags datatrafik kommer direkt via mobilen till molnet redan år 2018. Och Nokia, som i år slog på stort under mässan med återlanseringen av sin ikoniska mobiltelefon 3310, visar i sin ”Intelligence threat report” att antalet attacker mot smarta telefoner dubblerades under första halvåret 2016 och att smarta telefoner stod för 78 procent av attackerna mot mobila nätverk.

Efter mina dagar på MWC är det tyvärr smärtsamt uppenbart för mig att det inte går att göra en riktig säkerhetsspaning från eventet. Av den uppenbara anledningen att väldigt få aktörer väljer att lyfta fram och prata om säkerhet. Detta trots att ämnet borde vara det enskilt viktigaste på MWC, med tanke på det kraftigt ökade antalet hot som finns mot våra smarta telefoner.

Då inte tillverkarna eller branschen prioriterar säkerhet på årets konferens vill jag skicka med tre anledningar till varför svenska företag bör prioritera IT-säkerhet, och inte förlita sig på tillverkarnas ofta bristfälliga säkerhet.

1. DEN MÄNSKLIGA FAKTORN. Vår smarta telefon är en av få prylar där vi lagrar data som är både privat och arbetsrelaterad, men trots detta lägger vi lite vikt vid att skydda den.

Vad många företag inte tänker på är att telefonen är ett utmärkt sätt för kriminella att ta sig in på företagets nätverk och servrar. Anställdas smarta telefoner är tacksamma mål för attacker då den säkerhet som finns inbyggd i luren oftast är beroende av att den anställde regelbundet uppdaterar operativsystemet. Något som kan vara svårt för arbetsgivaren att hålla koll på. Cyberkriminella är väl medvetna om detta och är inte sena på att utnyttja det.

Bogdan Botezatu är IT-säkerhetsexpert på tekniksäkerhetsföretaget Bitdefender. Hans expertisområden är IT-attacker och säkerhet inom sakernas internet (IoT). Bogdan Botezatu har gett ut två böcker i ämnet, ”A history of malware” och ”Botnets 101”, samt böckerna ”Safe blogging guide”, med rekommendationer om att hålla sin blogg säker från attacker, och ”Securing wireless networks” om att skydda sitt hemnätverk från intrång. Läs mer om honom på *botezatu.info*.

Foto: GSMA

congress

2. OSÄKRA WIFI-UPPKOPPLINGAR. Vi lever i en tid då vi alltid på väg någonstans vilket gör att anställda ofta använder telefonen för att skicka mejl, ta ett konferenssamtal eller till och med skriva dokument på stående fot. Perfekt för den fria arbetskulturen, men vad många inte tänker på är den potentiella säkerhetsrisk som följer. Anställda kopplar ofta upp sig mot sitt hemnätverk, på fiket eller på flygplatsen.

Detta utan att tänka efter huruvida wifi är säkert eller inte, vilket snabbt och enkelt kan ge utomstående tillgång till telefonen och den data som skickas.

3. SÅRBARA APPAR. Smarta appar i alla dessa former har underlättat arbetslivet för många men för säkerhetsansvariga är det enorma ekosystemet av appar en ständig huvudvärk. Apparna är sårbara jämfört med de traditionella system som används ute på företag och de är många gånger inte byggda för traditionella säkerhetslösningar.

Att användaren inte heller uppdaterar apparna regelbundet gör det ännu svårare att skydda företagets mobila enheter även om utvecklarna gör säkerhetsuppdateringar.