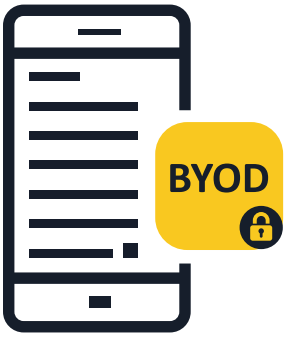
MALWARE PE DISPOZITIVELE MOBILE

IDEI ŞI SFATURI UTILE PENTRU COMPANII

1 Informaţi-vă personalul cu privire la riscurile mobile

- Dacă lucraţi de pe un dispozitiv mobil, liniile dintre utilizarea corporatistă şi cea personală se înceţoşează. Companiile pot fi grav afectate de un atac condus iniţial pe dispozitivul mobil al unei persoane. Un dispozitiv mobil este un computer şi trebuie protejat ca atare.



2 Implementaţi o politică corporatistă de tipul BYOD (folosiţi propriul dispozitiv)

- Angajaţii care îşi folosesc propriile dispozitive mobile pentru a accesa datele şi sistemele companiei (chiar dacă este vorba doar despre e-mail, calendar sau baza de date cu contacte) trebuie să respecte politicile companiei. Alegeţi cu grijă ce tehnologii se vor utiliza pentru a gestiona şi securiza dispozitivele mobile şi pentru a încuraja personalul să exercite atenţie.

3 Includeţi politicile privind securitatea mobilă în cadrul general privind securitatea

- Dacă un dispozitiv nu respectă politicile privind securitatea, conectarea acestuia la reţeaua corporaţiei şi accesul la datele corporaţiei nu trebuie permise. Companiile trebuie să aplice propriile soluţii de management al dispozitivelor mobile (MDM) sau de management al mobilităţii întreprinderii (EMM).
- În plus, este fundamental să instalaţi o soluţie de apărare împotriva ameninţărilor mobile. Aceasta va asigura vizibilitate îmbunătăţită şi conştientizarea contextuală a ameninţărilor la nivelul aplicaţiilor, reţelei şi sistemului de operare.

4 Aveţi grijă atunci când utilizaţi reţele publice Wi-Fi pentru a accesa datele companiei

- În general, reţelele publice Wi-Fi nu sunt sigure. Dacă un angajat accesează datele companiei folosind o conexiune gratuită Wi-Fi într-un aeroport sau o cafenea, datele pot fi expuse utilizatorilor rău intenţionaţi. În acest sens, se recomandă ca toate companiile să dezvolte politici de „utilizare eficientă”.

5 Actualizaţi-vă sistemele de operare şi aplicaţiile

- Recomandaţi personalului dvs. să descarce actualizările software pentru sistemul de operare al dispozitivului mobil de îndată ce acest lucru se solicită. În special pentru Android, căutaţi furnizorii de telefonie mobilă şi producătorii de telefoane mobile pentru a afla politica acestora privind actualizările. Având cele mai recente actualizări, nu numai că dispozitivul este mai sigur, dar şi funcţionează mai bine.

6 Instalaţi numai aplicaţii care provin din surse de încredere

- Companiile trebuie să permită numai instalarea aplicaţiilor din surse oficiale pe aceste dispozitive mobile care se conectează la reţeaua companiei. Opţional, luaţi în considerare construirea unui magazin de aplicaţii al companiei prin care utilizatorii finali pot accesa, descărca şi instala aplicaţii aprobate de companie. Consultaţi vânzătorul dvs. de soluţii de securitate pentru recomandări privind configurarea sau construiţi propriul magazin intern.

7 Prevenirea operaţiunii de jailbreaking

- Jailbreaking este procesul prin care se elimină limitările de securitate impuse de vânzătorul sistemului de operare, oferind acces complet la sistemul de operare şi funcţii. Efectuând o operaţiune de jailbreak pe dispozitivul dvs., securitatea acestuia poate fi redusă semnificativ, oferind breşe de securitate care nu erau aparente imediat. Dispozitivele cu acces la rădăcină nu trebuie permise în mediul companiei.

8 Luaţi în considerare alternative de stocare în cloud

- Utilizatorii de telefonie mobilă doresc deseori să acceseze documente importante nu numai de pe computerele de la locul de muncă, dar şi de pe telefoanele sau tablele private, în afara biroului. Companiile trebuie să ia în considerare dezvoltarea unor servicii sigure de stocare în cloud şi sincronizare a fişierelor pentru a răspunde la asemenea nevoi într-un mod sigur.

9 Încurajaţi personalul să instaleze o aplicaţie de securitate mobilă

- Toate sistemele de operare sunt supuse riscului de infecţie. Dacă este disponibilă, asiguraţi-vă că personalul utilizează o soluţie de securitate mobilă care detectează şi previne infecţia cu malware, spyware şi aplicaţiile rău intenţionate, precum şi alte funcţii care vă protejează confidenţialitatea, inclusiv funcţii anti-furt.

EUROPOL EC3 European Cybercrime Centre | POLIŢIA ROMÂNĂ | DICOT | CERT.RO | #MobileMalware