

Atenție la securitatea dispozitivelor mobile!

În prezent, dispozitivele mobile au ajuns să concureze computerele din punct de vedere al performanțelor și este de așteptat ca, în curând, să le și înlocuiască. Atât în mediul de afaceri cât și în viața particulară, comunicarea prin intermediul telefoanelor mobile este deja un lucru cât se poate de normal. Telefoanele mobile se manifestă deja de o vreme ca niște computere la purtător, ele putând stoca liste de contacte, documente Excel, muzică, filme, se poate naviga pe Internet, se pot face plăți bancare ș.a.m.d.

Malware pentru dispozitivele mobile

Este de așteptat ca dispozitivele mobile să devină cu timpul țintele preferate ale atacurilor informatice, în viitorul apropiat sau pe termen mediu. Multiplele posibilități de acces la Internet (Wi-Fi, GPRS- 3G,) precum și facilitățile de comunicare prin SMS, MMS sau conectarea prin Bluetooth vor oferi în continuare autorilor de malware oportunități pentru a ataca dispozitivele mobile. Furtul de date personale, infectarea sau blocarea telefonului, trimiterea de spam prin sms chiar și operațiuni care au drept consecință costuri suplimentare pentru utilizator sunt doar câteva din pericolele potențiale.

Principalii jucători pe piața telefoanelor mobile de ultimă generație (inteligente) încearcă să asigure din start securitatea dispozitivelor, dar o multitudine de amenințări nu pot fi tratate de aceștia pentru că nu dețin tehnologia și nici expertiza necesare. De exemplu mesajele de tip spam, atacurile de phishing și alte genuri de probleme de securitate nu pot fi combătute prin măsurile producătorilor de telefoane și de aceea specialiștii BitDefender recomandă insistent utilizarea unor aplicații specializate de securitate, pentru a putea beneficia de cea mai bună protecție împotriva amenințărilor informatice.

Mesajele nesolicitate și phishing-ul nu mai reprezintă o amenințare doar pentru stațiile de lucru. Volumul spam-ului prin intermediul dispozitivelor mobile, mai ales cel prin SMS este de așteptat să crească foarte mult în viitorul apropiat, dacă judecăm doar după sancțiunile recent primite de Vodafone România pentru această practică.

Tehnicile obișnuite de spam vizează acum și aplicațiile dispozitivele mobile ținând cont de faptul că toate modelele sunt echipate cu browsere, cum ar fi Safari, Opera sau Internet Explorer și clienți de poștă electronică.

Dispozitive furate/pierdute

Dispozitivele mobile pot fi cu ușurință pierdute sau furate, deci prezintă un risc mai ridicat decât în cazul PC-urilor de a pierde informațiile personale sau cele de business sau ca acestea să ajungă în mâinile unora care le vor folosi într-un scop criminal. Pentru a evita astfel de consecințe neplăcute, recomandăm ca informațiile personale, secrete sau nu, să nu ajungă pe device-uri mobile, sau să fie păstrate numai criptate și protejate de un antivirus (care ar putea detecta un eventual keylogger software).

Virusii dedicați dispozitivelor mobile

Distrația continuă în 2009 cu virusii dedicați telefoanelor mobile. Dispozitivele cu acces la Internet au trezit în mod special interesul specialiștilor în securitate IT. Virusii care se folosesc de vulnerabilități ale browser-elor vor deveni un lucru comun anul acesta.



Beneficiile oferite de soluția BitDefender Mobile Security:

1. Protecție permanentă împotriva virusilor
2. Scanare la cerere și dezinfectare de virusi
3. Consum redus de resurse
4. Actualizare facilă a produsului prin conectare la Internet

Răufăcătorii care vizează acum în primul rând computerele, se orientează deja și asupra dispozitivelor mobile. De curând, pentru prima oară în istorie, numărul celor care accesează Internetul de pe telefonul mobil a egalat numărul celor care fac acest lucru folosind PC-ul. Prin urmare, furnizorii de virusi, atacuri de tip phishing, mesaje spam, ș.a.m.d. vor avea din ce în ce mai multe motive să se orienteze și către dispozitivele mobile. BitDefender oferă utilizatorilor de smartphone-uri un produs destinat dispozitivelor mobile, BitDefender Mobile Security. Versiunea actuală a produsului poate fi instalată și utilizată pe orice dispozitiv (fie telefon mobil, fie PDA) care utilizează un sistem de operare fie Windows Mobile versiunea 5 sau 6, fie Symbian versiunile 7 sau 8.

Utilizatorii de dispozitive mobile, mai ales cei din mediul de business, dar nu numai, trebuie mai întâi să-și impună o anume „igienă a securității”. Pentru aceasta recomandăm:

- să definească și să activeze parole sau coduri PIN acolo unde este cazul;
- să instaleze un produs antivirus pe dispozitivul mobil propriu;
- să protejeze cu parole fișiere considerate „confidențiale” și stocate pe telefonul mobil.

De asemenea, având în vedere utilizarea dispozitivelor mobile și în interes de serviciu, devine vitală impunerea unor măsuri de securitate la nivelul companiilor, prin:

- stabilirea unor politici de folosire a unor documente sau fișiere de la birou pe telefonul mobil;
- monitorizarea respectării de către fiecare angajat a regulilor de securitate setate;
- stabilirea unor politici de securitate pentru conexiunile mobile sau de tip VPN la rețeaua firmei.

Toate aceste politici de securitate vor trebui actualizate frecvent având în vedere că în aceasta zonă lucrurile se schimbă cu o mare viteză.

În concluzie, amenințările informatice la adresa computerelor se vor manifesta din ce în ce mai mult și în cazul dispozitivelor mobile și, în plus, vor aduce și o serie de riscuri specifice doar acestei categorii. Telefoanele mobile sunt expuse suplimentar pentru că în cazul lor se folosește o gamă largă de sisteme de operare, fiecare cu vulnerabilitățile sale. Symbian, Windows Mobile, Blackberry OS de la RIM, iPhone OS de la Apple sunt fiecare dintre ele din ce în ce mai răspândite și, în plus, altele noi, ca de exemplu Android de la Google, recuperează constant teren. ☺