10 pasi esentiali pentru securitatea email Cand vine vorba de riscuri, e uimitor ca inca mai permitem trafic email in companii. Pe de alta parte, nici nu poate fi oprit. Astfel, f Urmand cateva principii de baza, nu exista nici un motiv pentru care traficul email legitim sa nu poata continua dinspre si inspre c Pasul 1: Stabilirea si promovarea unei politici robuste pentru email Nu serverele trimit email-uri, ci oamenii. Din acest motiv, e important ca toti angajatii unei organizatii sa inteleaga exact regulile d O politica buna este: clara, usor de interpretat; realistica, bazata pe toate aspectele afacerii, pentru a reflecta modul de lucru al co Pasul 2: Aflati impotriva cui va aparati Daca strategia de securitate pentru email nu acopera cel putin una din urmatoarele amenintari, atunci un atac este iminent: virus Pasul 3: Aveti grija ca apararea poate fi sustinuta O solutie de securitate pentru email care supraincarca departamentul IT si administratorii de email va esua eventual, si va irosi ta O solutie care poate fi sustinuta: foloseste tehnologia cea mai recenta, inclusiv filtrarea robusta a traficului si unelte de analiza; es Pasul 4: Aveti grija ca intregul trafic sa fie protejat Nu e o idee buna sa protejati doar traficul care intra in reteaua companiei, iar traficul dinspre companie si cel intern sa fie comple Pasul 5: Alegeti optiunea de instalare corecta Solutiile de securitate pentru email sunt disponibile in trei variante, fiecare cu avantaje si dezavantaje. Solutiile software sunt potr Organizatiile mici prefera servicii terte sau dispozitive, pe cand companiile mari aleg de obicei un model pe nivele, cu dispozitive Pasul 6: Inchideti fereastra pentru zero-day Solutiile antivirus si antispyware sunt bune pentru protectia impotriva amenintarilor cunoscute. Dar ce opreste un virus nou sa int Pasul 7: Ganditi in viitor Amenintarile impotriva companiei sunt intr-o schimbare continua. Nu vreti sa investiti intr-o tehnologie care va fi depasita atunci c Pasul 8: Monitorizati traficul si performantele retelei Nu puteti proteja ce nu puteti vedea. Folositi rapoarte pentru a observa comportamentul traficului de email-uri si problemele de pe Pasul 9: Nu uitati imaginile Nu toate mesajele nedorite sunt text. Imaginile indecente, ilegale sau neplacute pot deranja angajatii. Materialele confidentiale al Pasul 10: Investiti in conformitate Noile reglementari pentru raporturi financiare si protectia informatiilor poate pune presiune mare pe departamentul IT. Gateway-u Sursa: ComputerWorld Securitate IT

http://www.securizare.ro Powered by Joomla! Generat: 10 September, 2010, 05:07