SÃ©curitÃ©: Le social engineering : un nouveau dÃ©fi pour les RSSI
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 23/11/2011 11:30:00

La sÃ©curitÃ© informatique demeure lâ□□une des prÃ©occupations majeures des entreprises. En effet, la cyber criminalitÃ© Ã©crit chaque jour une nouvelle page en mettant en avant de nombreuses failles.

Les exemples ne manquent pas. Parmi lâ□□ensemble des actes de malveillances menÃ©es par les cybercriminels, nous assistons depuis peu Ã la montÃ©e en puissance dâ□□une nouvelle forme de menace appelÃ©e Â« social engineering Â». Mais quâ□□entend-on prÃ©cisÃ©ment sous cette dÃ©finition ?. **Nicolas DUBOIS** - Auditeur technique, expert du Cybercrime - SDN International& Cyberprotect nous en dit plus.

Le social engineering, aussi nommÃ© Â« ingÃ©nierie sociale Â», a pour but dâ□□obtenir de la part de sa victime une action ou une information demandÃ©e. Les actions peuvent Ãªtre de dÃ©sactiver un antivirus sur un poste ou dâ□□effectuer un virement bancaire comme ce fut le cas en Aout dernier contre le groupe Quick et Scor. Les informations sont souvent de nature confidentielle, comme les informations sur un projet en cours, les identifiants de connexion, ou lâ□□agenda du PrÃ©sident.

Le social engineering est une forme d'acquisition dÃ©loyale d'information et d'escroquerie. Cette pratique exploite les failles humaines et sociales de la structure cible, Ã laquelle est liÃ©e le systÃ¨me informatique visÃ©. Utilisant ses connaissances, le hacker abuse de la confiance, de l'ignorance ou de la crÃ©dulitÃ© des personnes pour arriver Ã ses fins. Le social engineering est aussi appelÃ©e processus Â« d'Ã©litisation Â». Ce terme est souvent utilisÃ© en informatique pour dÃ©signer un processus d'approche relationnel frauduleux.

Cette nouvelle menace est donc une forme trÃ¨s complexe Ã apprÃ©hender. GÃ©nÃ©ralement, on distingue diffÃ©rentes formes de social engineering : lettre, tÃ©lÃ©phoneâ□¦ mais le plus souvent le mail est utilisÃ©. Il est donc important que lâ□□entreprise soit sensibilisÃ©e Ã ces pratiques et forme ses collaborateurs. De maniÃ¨re gÃ©nÃ©rale, de toutes les tentatives dâ□□attaques, lâ□□ingÃ©nierie sociale est la plus performante, car elle recouvre plusieurs formes et sâ□□adresse Ã des utilisateurs variÃ©s et non sensibilisÃ©s Ã cette menace.

Un hacker pourra, par exemple, chercher Ã obtenir les logins des collaborateurs d'une entreprise en se prÃ©sentant comme le responsable de lâ□□administration du SI... Il pourra utiliser le nom des responsables hiÃ©rarchiques pour justifier de sa dÃ©marcheâ□¦ Tous ces Ã©lÃ©ments scÃ©narisÃ©s permettent de mettre la personne sollicitÃ©e en confiance. Ainsi, un test rÃ©alisÃ© auprÃ¨s de 17 groupes amÃ©ricains a permis de dÃ©montrer que la majoritÃ© des employÃ©s contactÃ©s communiquent leurs mots de passe. Un point intÃ©ressant de cette Ã©tude montre Ã©galement que les femmes semblent mieux rÃ©sister aux diffÃ©rentes sollicitations.

Lâ□□affaire **Hacker Croll** est Ã©galement un bon exemple et montre quâ□□il nâ□□est plus nÃ©cessaire de disposer de compÃ©tences informatiques pointues pour se transformer en cyber criminel. Ainsi, ce jeune pirate a pu usurper l'identitÃ© de Barack Obama ou encore de Britney Spears sur leurs profils Twitter. Il a Ã©galement pu mettre la main sur des documents confidentiels de Twitterâ□¦

Toutes les entreprises doivent donc prendre en compte ce nouveau danger et dÃ©ployer des stratÃ©gies de formation pour lutter activement contre ce phÃ©nomÃ¨ne. Les collaborateurs doivent pouvoir anticiper et ne pas se laisser abuser par de tels stratagÃ¨mes. Sâ□□en protÃ©ger, nÃ©cessite dâ□□ajouter aux procÃ©dures classiques de sÃ©curitÃ© informatique, la formation du personnel. Câ□□est Ã cette condition que les entreprises pourront se prÃ©munir de cette nouvelle menace.