SAMPLE – CyberSecurity

The Changing Face of Cyber Crime – New Threats You Should be Aware Of

The importance of cyber security for companies cannot be emphasized enough. A big part of preparing for possible future attacks is to be aware of not just the existing threats, but also new ones. Keep in mind that cyber crime is as dynamic as your interactive website. Only when you understand what you are up against can you incorporate suitable measures to remove vulnerabilities. Here's a look at the changing face of cyber crime.

Hacktivism

Nothing explains hacktivism better than WikiLeaks, which threatened to blow the lid off political scandals, and made the Obama Administration, among others, break into a sweat. When the likes of MasterCard, PayPal, Visa and Amazon came under pressure to suspend payment services to WikiLeaks, 'hacktivists' launched DOS (denial-of-service) attacks against them in a show of support for WikiLeaks and its Australian founder Julian Assange.

Hacktivism includes any form of security breach and cyber attack, the motive for which is not monetary gain, but a disagreement with the decisions and practices of the targeted websites.

Sample another case of hacktivism, this time involving RIAA (Recording Industry Association of America) and MPAA (Motion Picture Association of America), against whom the members of imageboard site 4Chan launched DDOS (distributed denial of service) attacks. The retaliation had to do with the RIAA's and MPAA's role in shutting down The Pirate Bay, a bit-torrent site and a haven for illegal downloading.

The threat of hacktivism is alive and real – even if you believe that there is no motive for 'cyber activists' to target your company's website, it is advisable to establish the necessary cyber-security measures to combat this threat effectively.

Clickjacking

If your company maintains a Facebook presence, then 'clickjacking' may sound familiar. In simple words, clickjacking is a form of cyber attack where the hacker uses an invisible layer over the embedded web content (this could be an image, video or button) to intercept and 'hijack' you to a mirror website and mine information from you. You will be unaware that you have been routed to another webpage, and this will cost you big, in terms of divulging sensitive information that can be used for malicious intent.

Cross Site Scripting

A threat to webpages that contain dynamic content, cross site scripting is a form of cyber attack that is targeting commercial websites across the world. Once the attacker figures out that an application on your site is defenseless against cross site scripting, the attacker will formulate and launch an attack, which may include (a) making changes to user settings (b) hijacking accounts (c) cookie theft (d) false advertising. The users can also be connected to a server that the attacker has chosen, which in all likelihood will be a malicious one.

Vulnerability of Mobile Devices

Tablet PCs and smartphones have revolutionized the way we use technology. These devices are fast becoming a very integral part of our everyday lives. Unfortunately, with the good comes the bad; and cyber criminals are increasingly targeting mobile devices, including tablets and digital wallets. The malicious intent in this case is almost always linked to financial gain. Online banking through smartphones is one instance where a malicious real-time attack can result in significant monetary losses. The services that are hosted on popular gadgets, like the iPhone or Android based devices, can be infected with corrupt software or used for access to sensitive information.

Cloud Computing Loopholes

You may have experienced the convenience and cost-savings of cloud computing. But here's a bit of bad news – cyber crime is all set to make its way across cloud-based applications and services. A more recent case of cloud-related security compromise was in the form of a malware named "Trojan-Dropper.Win32.Drooptroop.jpa" that was detected in Rapidshare, the extremely popular cloud-based file-hosting website. A concerning feature about this malware was that it was able to bypass traditional cyber security filters by not being visible in the Rapidshare link's body.

Sophisticated Attacks on a Specific Target

Stuxnet is a computer worm that made an appearance in 2010, and showed how malware can be used to launch cyber attacks on a global scale. Targeting computer systems that use Siemens software, this worm was tailored to attack an Iranian nuclear power plant. China's 'Aurora' attack targeting Google is yet another indication that cyber warfare, launched by nations, can pose a big threat to companies on the receiving end of the attack.

With the right cyber-security measures, you can enjoy peace of mind, prevent any potentially harmful attack and avoid embarrassments. In this regard, it is advisable to engage the services of a reliable cyber-security firm that can address all such concerns of your business.