Approaching Security Awareness the Smart Way with Threat Intelligence

Posted on August 20, 2018



While digitalization has brought many benefits like faster and easier communication, there are also disadvantages that businesses must be ready to face as a side effect — most notably, cybersecurity threats. Whois API Inc. CEO founder Jonathan Zhang has recently appeared as a guest expert on The Security Awareness Company's website discussing that tension and the synergies existing between threat intelligence and security awareness. Some of the main points covered are summarized below.

Threat Intelligence Goes First

Until you know what your business' most salient vulnerabilities are, it's hard to put a smart cybersecurity roadmap together. That's why threat intelligence (TI) is a vital start which provides guidance in the form of integrated evidence-based data regarding the weak spots present within a company's IT infrastructure and online assets — flagging poor security configurations and suggesting areas for improvement. Building on TI insights, security professionals can stay one step ahead of cybercriminals and anticipate what cyber threats are most likely to look like.

Spoofing

Is the business trustworthy? Are the people really who they claim to be? TI allows you to collect information about domain owners — names, email, and physical addresses — from **whois databases** and compare it with what is claimed on websites or business communications to detect impersonators.

Malware

Multiple forms of ransomware, trojans, and viruses emerge every day, and security professionals can stay on top with a threat intelligence platform linked to the major malware databases that collect details about new attacks as they spread.

Hacking

Security misconfigurations is a dream come true for hackers looking to forge websites and collect sensitive data from visitors. As part of a TI analysis, security specialists can make sure this does not happen by identifying the gaps in their encryption capabilities — be it SSL certificates, HTTPS enforcement, or something else.

Security Awareness Remains Essential Though

However, flagging threats is only the first step. Even after reinforcing the weak links of infrastructure and systems, there is still a sizeable number of attacks and scams slipping through, and those can be tackled through security awareness initiatives — e.g., training, learning modules, and educational security newsletters.

Do you want to find out more about the benefits of threat intelligence and its synergies with security awareness? You can check the full version of this post or contact us at general@whoisxmlapi.com.