10 ESSENTIAL CYBERSECURITY TIPS FOR BUSINESSES

Telecommunications providers around the world hold a wealth of cybersecurity data from their vast networks and customer bases. Members of the Global Telco Security Alliance offer 10 key insights businesses and other organizations need to know about the state of cybersecurity.

SOCIAL ENGINEERING IS THE TOP TACTIC

Social engineering was the top method of compromise in 2018. 60% of breach investigations can attribute successful social engineering as the conduit to initial point of entry.

100% OF WEB APPS ARE VULNERABLE

100% of the web applications tested possessed at least one vulnerability, with the median number of vulnerabilities rising to 15, up from 11 in 2017.

SEXTORTION GAINS GROUND

Sextortion email campaigns, designed to dupe victims into paying large ransoms by playing on fears that compromising videos exist on the recipient, rose toward the end of 2018 to account for 10% of all spam analyzed.

CRYPTOJACKING MALWARE SKYROCKETS

A steep year-over-year increase of 1,250% was observed in cryptojacking malware. Used to covertly place legitimate JavaScript coin miners on websites or infect carrier-grade routers, cryptojacking malware illegally mines cryptocurrency for cybercriminals using the computing resources of unsuspecting victims.

ORGANIZATIONS ARE NOT RISK DRIVEN

50% of companies have programs that are not risk driven and are not integrated with overall security goals. As for incident response coordination capabilities, the number increases to 70%.

COMPANIES ARE MORE VULNERABLE THAN THEY THINK

Only 1 out of 3 companies is communicating with employees about the dangers of social engineering tactics including suspicious emails.

IT SECURITY INVOLVEMENT IS DELAYED

Almost 20% of IT security professionals get involved in cloud, mobility and IoT projects only after deployment. Getting involved this late in the game can be risky business, paving the way for hackers to access your network.

BEWARE OF ANDROID MOBILE APPS

Out of 2,000 applications selected on an arbitrary basis, 142 applications were malicious and remained 47.54 days (average) available in the market from their first upload. Furthermore, a total of 173 vulnerabilities of varying severity have been found in Android in the second quarter of 2018.

APP DETECTION AND REMEDIATION

Malicious applications detected by less than 5 antivirus engines have a longer market shelf life, with some staying in app stores for up to 100 days. While Google Play removed 45,000 apps, antivirus engines only detected 2% of them.

ADOBE IS A PRIME MALWARE VECTOR

Among the 25 companies with the highest number of CVEs, Adobe software featured the most vulnerabilities (292 CVEs in total). Almost all of the them correspond to their Acrobat Reader (239 CVEs assigned) which is commonly used to access PDFs.

AT&T Cybersecurity · etisalat digital · Trustwave® a Singtel company · SoftBank · Eleven Paths Telefonica CYBER SECURITY UNIT

Sources: 2019 Trustwave Global Security Report, AT&T Cybersecurity Insights Report V8.5, Telefonica Global Security Report