Technology & Innovation

The Changing Face of Crime: Cybersecurity Best Practices

NEWS

CIANJ Opposes Minimum Wage Hike
Read more →

Health Exchange Bills Debated
Read more →

Assembly Passes Construction Permit Extension
Read more →

New Budget Includes Income Tax Cut
Read more →

VIEW ALL NEWS->

>>POST YOUR OWN NEWS

The Changing Face of Crime: Cybersecurity Best Practices

by: Martin C. Daks
March 9, 2018

CYBERCRIME IS ON THE RISE, draining about $500 billion a year from businesses worldwide. Last year's massive data breach of credit reporting agency Equifax exposed the names, Social Security numbers, birth dates and addresses of an estimated 143 million people to hackers.

A 2013 breach of retail giant Target's systems affected more than 41 million customer payment card accounts and exposed contact information for more than 60 million customers. Most recently, two new threats—Meltdown and Spectre—exploit flaws built into just about every computer chip built since the mid-1990s.

The threat is real and growing, and that's why cybersecurity expert Dr. Eric Cole released a book this February, ***Online Danger: How to Protect Yourself and Your Loved Ones From the Evil Side of the Internet.***

Cole, who was cybersecurity commissioner for President Barack Obama and has a Ph.D. in Information Technology, is CEO of Reston, Virginia-based Secure Anchor Consulting. In addition, Cole is the former chief technology officer of computer security company McAfee, and former chief scientist of aerospace, defense and technology giant Lockheed Martin.

Here are Dr. Cole's cybersecurity best practices, and his insights on how to safeguard business data and customer information from the bad guys.

Identifying Vulnerabilities. "Hackers trick employees to open an e-mail attachment or click on a malicious link and expose an otherwise protected database. Companies should try to limit the ways that their employees can access the Internet to limit exposure to cybercrime."

Protecting Company Data. "Some companies give employees two computers: one to surf the Web and check e-mail, and a second one that is limited to doing their work on a secure, private network. That's what we did when I was an analyst with the CIA in the late 1980s."

Incentivizing a Culture of Cyber Safety. "Companies can reinforce good habits by making the security matrix a Key Performance Indicator that's part of an employee's bonus. Other firms opt to limit functionality—they don't allow e-mail attachments, and don't allow embeddable links—but that can reduce employee effectiveness."

Testing Breach Risks. "Small- to medium-sized retailers—even ones that engage in e-commerce—aren't a big target, because they usually just pass through credit card information to third-party processors without storing the data themselves. If a hacker goes after a retailer, it's likely to be a big operation that has its own database of consumers' personal information."

Knowing Your Business is a Target. "Any business that stores a large volume of personal data is a potential target. This includes credit card companies, banks and mortgage companies. Technology companies are also at risk, especially from China-based hackers, since the government there is looking to beef up its tech knowledge and ability."

Presenting Business Best Practices. "A server with critical data should never be accessible from the Internet. If you're encrypting data, be sure to store the key on a separate, secured server. Any system that can access the Internet, say for e-mails, should have 'application whitelisting' installed."

Whitelisting. "With a digital index of approved software applications that are allowed to be present and active on your computer system, an attacker can't get his or her malware or virus to run on your system."

Preventing Breaches. "The Equifax attack, for example, was easily preventable. The company had a server that could be accessed from the Internet, but it was missing safeguards. Equifax and similar businesses often spend millions of dollars on things like firewalls and monitoring systems. But then they don't employ enough people to monitor

the threat messages. Analysts are overwhelmed by alerts and begin to ignore some of them, and by the time they recognize that their security has been penetrated, it's too late."

Closing Loopholes in Cyber Defense. "Equifax and other large companies should have an updated asset inventory that outlines what systems are visible from the Internet, and how they are configured: are they locked down and secured and updated, or are they vulnerable? They also need to manage and control any changes to the system. So, if a software or hardware engineer modifies the system or changes any components, they'll first have to go through a security process that will enable them to understand what kind of impact the changes will have on the entire organization and its systems."

Using Applications that Expose Systems to Hacking. "Web browsers and e-mail clients are the biggest risks. Everyone trusts them and thinks their communications are secure. People go to a Web site, think it's safe, and they start clicking when they shouldn't. Instead, you should only go to known, trusted sites."

Increasing the Odds of a Breach. "Keep away from search engine results, because many results are malicious. Also, people get e-mails with links that look legitimate, but may not be. Don't open attachments or click on links unless you're sure they're safe."

Identifying the Origins of Cyberattacks. "Many times, the hackers have some connection to governments in mainland China, Russia, or North Korea. The attacks are very organized—these are too sophisticated for rogue criminals. One group, the Russian 'business network' has close ties to the Russian Army, with at least 3,000 professional hackers as employees."

Assessing the Continuing Threat. "The bad guys are ahead because their job is easier—they only have to find a single vulnerability in a system and they're in. The good guys have to find and defend all vulnerabilities—one weak spot, and your adversary is in."

VIEW ALL FEATURED ARTICLES

South 61 Paramus Rd. Paramus, New Jersey 07652 • Phone: 201-368-2100 • Fax: 201-368-3438