Aziksa

Delivering CyberSecurity Awareness training for companies worldwide.

March 2017

News Updates

Aziksa is a leading provider of learning delivery systems whose sought-after CyberSecurity Awareness course is arming employees with the information to protect company assets. You are receiving this newsletter because of your interest in learning about cyber security – threats, breaches, and how your organization can take an active role in preventing them from harming your organization. In this newsletter, you will be up to date on real threats emerging in the news.

Dangerous W-2 Phishing Scam Evolving

The Internal Revenue Service, state tax agencies and the tax industry issued an urgent alert to all employers that the Form W-2 email phishing scam has evolved beyond the corporate world and is spreading to other sectors, including school districts, tribal organizations and nonprofits.

“This is one of the most dangerous email phishing scams we’ve seen in a long time. It can result in the large-scale theft of sensitive data that criminals can use to commit various crimes, including filing fraudulent tax returns. We need everyone’s help to turn the tide against this scheme,” said IRS Commissioner John Koskinen.

https://www.irs.gov/uac/dangerous-w-2-phishing-scam-evolving-targeting-schools-restaurants-hospitals-tribal-groups-and-others

Cloudbleed

Last Week Google's Project Zero shared with industry that Cloudflare (a major provider of a content delivery network, Internet security services, and distributed domain name server services) was leaking sensitive information online. The company has patched the memory leak bug responsible (the flaw is being called "Cloudbleed"). Popular services (said to include Uber and Fitbit) use Cloudflare.

Since data have been leaking for some time, many researchers are advising users to assume their credentials have been exposed, and, of course, to change them.

MySQL Ransomware

Internet-facing instances of the popular MySQL information store are being targeted by attackers following similar attacks on insecure databases earlier this year. Security vendor GuardiCore this month spotted hundreds of attacks emanating from a Dutch web hosting company.

The attack itself relies on brute-forcing or guessing the root password for MySQL instances. If the attacker gets in to the MySQL database, a new table called "WARNING" with contact details for a ransom payment is added. In a variant of the attack, the ransom note table is called "PLEASE_READ". After the ransom note tables are created, the attacker then deletes all databases found on the compromised server. *(continued on next page)*

http://www.networkworld.com/article/3174306/security/ransomware-attacks-targeted-hundreds-of-mysql-databases.html

News Updates

MySQL Ransomware (cont.)

Teams should check the following on their MySQL installations:

- update the password plugin;
- set a password for the root account and change it every 90 days;
- remove root accounts that are accessible from outside the local host;
- remove anonymous-user accounts;
- remove the test database and privileges that permit anyone to access databases, and;
- avoid naming your databases starting with test_.

About Aziksa

Aziksa
940 Stewart Drive #205
Sunnyvale, CA 95070
Phone: 408-647-3010

http://www.aziksa.com

Aziksa is an industry leader in delivering blended learning solutions for Web and mobile-based training, education, and information solutions across the globe.