Enterprises fall behind on protecting against phishing, detecting breaches

http://www.csoonline.com/article/3061398/techology-business/enterprises-fall-behind-on-protecting-against-phishing-detecting-breaches.html

The ninth annual Verizon Data Breach Report came out this morning with bad news on multiple fronts

By Maria Korolov

CSO | Apr 26, 2016 4:32 AM PT

The ninth annual Verizon Data Breach Report came out this morning with bad news on multiple fronts, including click-through rates on phishing messages, how long it takes companies to detect breaches, and even whether companies spot the breaches at all.

Phishing emails continued to be a primary starting point for attacks, said Bryan Sartin, executive director, global security services at Verizon.

If enterprises want to understand how they can better invest in security defenses, build the necessary

The number of phishing email messages that were opened hit 30 percent in this year's report, up from 23 percent last year.

In addition, 12 percent of users don't just open the email but open the attachment as well, while 11 percent follow links in the email to online forms where they then input sensitive data such as login credentials.

The median time for the first user of a phishing campaign to open the malicious email was 1 minute, 40 seconds and the median time to the first click on the attachment was 3 minutes, 45 seconds.

The vast majority of the attacks, or 89 percent, were by financially-motivated crime syndicates, and the other 9 percent by state-affiliated actors.

Another problem that continues to plague enterprises is the lack of basic two-factor authentication, said Sartin. "It would mitigate an entire swathe of these breaches."

In fact, 63 percent of all breaches included the use of stolen credentials, up from 51 percent in last year's report.

Sartin suggested that enterprises might be getting buried in all the complexity of operational security management, or be too driven by compliance.

"Sometimes people get lost and can't see the forest through the trees," he said.

Then, once the attacker is in the system, enterprises are actually getting worse at detecting the problem.

In 92 percent of breaches, it took attackers just minutes to get into a company after the first attempt, with 30 percent able to exfiltrate the first data within hours, and another 68 percent able to get data out within days. But the number of enterprises that were able to spot a breach as it was happening in "days or less" was less than 25 percent.

In fact, the gap between the time to compromise and the time to discovery rose from 62 percent in last year's report to 84 percent this year.

In fact, the number of breaches detected internally, or via fraud detection mechanisms such as those in the credit card industry, have also fallen. Instead, most breaches are now detected by law enforcement authorities or other third parties.

"Third-party detection and law enforcement collaboration is getting better," said Sartin.

Once security experts take down one command and control server, for example, they may find that the same infrastructure was used to go after a number of victims. They also spot sensitive information as it shows up for sale on the dark web, he said.