6-CSO Online-How to protect

News

How to protect your company from an eBay-like breach

Experts recommend a number of defensive tactics ranging from employee education to monitoring of credential use on the network

OnInnovation (CC BY-ND 2.0)

The eBay database breach that led to the theft of customers' passwords and personal information started with the compromise of employee login credentials, a reminder that companies should check the safeguards in place for protecting such critical information.

EBay said Wednesday that a "small number" of employee credentials were compromised, which led to unauthorized access to the corporate network. The company has 145 million customers, but eBay did not say how many were affected by the breach. *[Diminish]*

"Anytime you get your hands on an account that has insider access, you've just made your job a lot easier as an attacker," Jonathan Sander, strategy and research officer at STEALTHbits Technologies, said.

EBay did not say how the credentials were stolen, but the database was breached between late February and early March. *[Deny]* The stolen data included customers' name, encrypted password, email address, physical address, phone number and date of birth. No financial data was stolen.

Employees can have their credentials stolen in many ways, such as using the same user name and password on a website that's compromised.

Employees could also become victims of phishing attacks or have their laptop infected with malware that logs keystrokes and sends the information back to the hacker's server.

As a matter of corporate policy, employees should be advised never to use their work credentials for logging into websites. Such advise falls under the category of employee education, which is the most effective non-technical form of security.

“The best line of defense, absolutely, is education,” Sander said. “This is something that I don’t think enough companies take seriously.” *[Disappointment]*

Other defensive mechanisms against credential theft include the use of two-factor authentication, such as a physical token that generates a one-time PIN for logging in, Jaime Blasco, malware researcher and labs director at AlienVault, said.

“That’s the easiest way,” Blasco said. “Even if they (hackers) steal your password, they’ll still need the physical token.”

Blasco has seen an increase in network break-ins that start with the theft of employee credentials. The uptick is likely the result of companies installing better technology to prevent breaching a system directly over the Internet.

“The weakest link is the user, and in this case, that’s the employee,” Blasco said. “So, we’re going to see more and more breaches and compromises tied to credentials of employees.”

One way hackers will steal corporate credentials is by planting malware on an employee’s personal laptop, which is then used to log into the corporate network. Employees should be told to access the network only with laptops secured by their employer, Blasco said.

Companies that monitor employee activity on the network are in the best position to spot unusual activity with a particular set of credentials. A red flag would be an employee’s credentials being used to access areas not normally visited by the worker.

“You should see the services people are using and establish baselines and patterns around that, so you can tell what’s normal and what’s not,” Sander said.

The fact that eBay did not discover the breach for roughly two months points to another common problem. Companies often do not know they’ve been compromised for weeks after the breach.

A study of 691 data breaches over the last year found that the median time between intrusion and detection was roughly three months, according to security vendor Trustwave. The median time between discovery and containment was seven days.

EBay is the latest of several companies that have suffered high-profile breaches recently. Others include retailers Target and Neiman Marcus.

Experts have said that the Target breach, which resulted in the theft of millions of credit-card numbers, could end up costing the company more than $1 billion.

Next read this