One in three enterprises can’t protect themselves from data breaches

Ponemon says that a third of companies do not believe they could fend off a data-stealing cyberattack in 2019.

By Charlie Osborne for Zero Day | February 13, 2019 -- 13:00 GMT (05:00 PST) |

One in three enterprise companies do not believe they have the capabilities required to fend off a cyberattack leading to a data breach, research suggests.

According to a survey involving over 600 cybersecurity professionals in business conducted by Balbix on behalf of the Ponemon Institute, organizations are having severe difficulties in implementing modern security solutions to keep their information protected.

The survey, published on Wednesday, suggests that vulnerability patch management, alongside finding the skilled staff required to maintain even basic bug resolution procedures are the main barriers to adequate security against data breaches.

In total, 85 percent of respondents said that staffing levels were inadequate to maintain a "strong cybersecurity posture," and only 15 percent of those surveyed said their patching efforts were "highly effective."

Figure 1. How confident are you that your organization can avoid a data breach?

A common problem many corporations faced in relation to patch management is ascertaining which vulnerabilities may impact them, especially when a lack of visibility into ever-more complex networks proves to be an obstacle.

Scanning is also a barrier to finding relevant vulnerabilities to an enterprise. In total, 69 percent of those surveyed they scan their systems for weaknesses once a month -- or less -- and 49 percent scan only on an ad-hoc or quarterly basis.

When it comes to patching processes, only 49 percent of respondents said their company does reliably complete up-to-date patching requirements.

In total, 67 percent of respondents said they do not have neither the time or the resources to mitigate every bug which could be exploited to give attackers access to sensitive information, and 63 percent say that the "inability to act on a large number of resulting alerts and actions" is a security problem.

When asked what tools they would like to have in their patch arsenal, respondents said:

- Automatically discover unmanaged assets (70 percent)
- Analyze vulnerabilities in IoT, BYOD and third-party systems (64 percent)
- Analyze both unpatched systems and other attack vectors (60 percent)
- Receive a risk-based and prioritized list of actions (56 percent)
- Receive prescriptive fixes per recommended action (52 percent)

"From this research, it is clear that most enterprises recognize not only are they under-resourced in finding and managing their vulnerabilities, but they also have gaps around assessing the risk and getting full visibility across their IT assets," said Larry Ponemon, founder and chairman of the Ponemon Institute, "which no doubt led to that low confidence vote in their ability to avoid a data breach."

According to Cisco's SMB Cybersecurity Report, the average SMB faces costs of up to $2.5 million after a data breach. However, when data breaches impact millions of customers -- such as in Marriott's case -- the tab may end up running into the billions.