Business needs to shift budget to relevant security, says Verizon

Warwick Ashford Thursday 15 May 2014 09:25

Many businesses are failing to invest in blocking the threats that are actually hitting them, says Eddie Schwartz, vice-president of global security solutions, Verizon.

“This is because most of their budget is still being spent on traditional perimeter defences, which means there is little left over for anything else,” he told Computer Weekly.

“Most organisations adopt a ‘peanut butter approach’ of spreading defences evenly across their entire IT estate, instead of investing in systems to block the kinds of attack most likely to hit them,” he said.

Verizon's *2014 Data Breach Investigations Report* revealed that businesses need to focus on only a few attack methods to cover most cyber attacks that affect them.

The firm’s researchers found that, while no organisation is immune from attack, 92% of cyber attacks in the past 10 years can be linked to just nine basic attack patterns.

Of these, most companies have to face only two or four types of threat, depending on the industry vertical, which determines the kind of data they hold and the types of attacks and attackers they face.

While financial firms need to prioritise web application attacks and payment card skimming, for example, retailers need to focus on point of sale intrusions and denial of service attacks.

“This is the coolest report of its kind,” said Schwartz. “The data enables organisations to identify the most prevalent kinds of attacks on their industry and the most appropriate security controls to deploy.”

“Leading organisations are starting with who is likely to attack them and how that relates to the business and what they need to protect as a threat model for identifying the most effective controls,” he said.

Effective defence

This is a much better approach, he said, than spending vast sums of money creating a semblance of security that attackers can easily bypass.

This is a huge problem, said Schwartz, because once an attacker in inside a network, in most organisations they are able to move laterally without difficulty and without being detected for some time.

“Historically, security has been about understanding what is bad and looking for that, but it needs to be more about understanding what is good so we can identify meaningful differences,” he said.

This means organisations need to look at things like network dynamics and baselining, anomaly detection and big data analytics to help identify malicious activity, said Schwartz.

Security opportunity

“Once they start doing things they become more visible if you know what you are looking for, which presents a huge opportunity that the security industry needs to get better at exploiting,” he said.

Schwartz predicts that, in the next three years, organisations will move towards employing service providers who can undertake most of their cyber defence for them.

“Very few organisations have the resources to develop the necessary capabilities in-house, so they will look instead to service providers who can do it at a reasonable cost through economies of scale,” he said.

While organisations will continue to do basic security hygiene, vulnerability management and governance, risk and compliance, they will move out of more complex areas.

The areas most likely to moved over to specialist service providers, he said, include cyber operations, cyber attack management, cyber intelligence, and cyber investigations and forensics.

Most cyber attacks use only three methods, Verizon breach report shows

Warwick Ashford Wednesday 23 April 2014 08:00

Businesses need to focus on only a few attack methods to cover most cyber attacks, Verizon's *2014 Data Breach Investigations Report* has revealed.

The firm’s researchers found that while no organisation is immune from attack, 92% of cyber attacks in the past 10 years can be linked to just nine basic attack patterns.

Of these, most companies have to face only between two and four, according to Dave Ostertag, global investigations manager at Verizon.

“By identifying the threats that enable most attacks for each sector, this report enables firms to have a more focused and effective approach to fighting cyber threats,” he told Computer Weekly.

“This enables companies to draw up a strategy, prioritise security investments, see what will give the best returns, identify trends and predict where things are going to identify potential targets,” said Ostertag.

Top threat patterns identified by the report

- Malware aimed at gaining control of systems
- Insider/privilege misuse
- Physical theft or loss
- Web app attacks
- Denial of service attacks
- Cyber espionage
- Point-of-sale intrusions
- Payment card skimmers
- Miscellaneous errors such as sending an email to the wrong person

A clear trend that has emerged in the past year, he said, is that attackers are increasingly targeting data about business deals, such as mergers and acquisitions, property deals, purchase bids and contracts.

Researchers found that, on average, just three threat patterns cover 72% of the security incidents in any industry.

“The report enables each industry to drill down into the threats specific to that industry and what is effective to detect and prevent those attacks,” said Ostertag.

For example, point of sale intrusions, denial of service attacks and web application attacks are responsible for 76% of cyber security incidents in the retail industry.

Similarly, by investing in defences around web application attacks, payment card duplication or skimming and denial of service attacks, financial services firms could cover 75% of cyber security incidents.

Big data analytics can reduce security risk

While most organisations are failing to keep up with cyber crime, the latest breach report shows that by applying big data analytics to security risk management, they can turn the tide, according to Verizon.

Specifically, this approach can help organisations reduce the time it takes to identify that a breach has taken place, thereby reducing the time attackers are able to exfiltrate data undetected.

The report shows that cyber espionage continues to increase, with more than 500 incidents representing a more than threefold increase compared with the 2013 report.

Although the increase is partly due to a bigger data set, Ostertag said reports of cyber espionage have increased steadily since 2007, with these attacks tending to be the most complex and diverse.

92% of cyber attacks in the past 10 years can be linked to just nine basic attack patterns

As in 2013, China continues to lead as the site of the most cyber espionage activity; but other regions of the world are represented, including Eastern Europe with more than 20%.

For the first time, the report examines distributed denial of service (DDoS) attacks that are aimed at making networks and systems inaccessible so that, for example, a website is rendered useless.

They are common to the financial services, retail, professional, information and public sector industries. The report points out that DDoS attacks have grown stronger year-over-year for the past three years.

According to the report, the use of stolen and/or misused user names and passwords continues to be the top way for attackers to gain access to information.

Two out of three breaches exploit weak or stolen passwords, making a case for strong two-factor authentication.

The report notes that the number of large retail point-of-sale (POS) attacks continue to trend downward, exhibiting the same trend since 2011.

Industries commonly hit by POS intrusions are restaurants, hotels, grocery stores and other brick-and-mortar retailers, where intruders attempt to capture payment card data.

While POS breaches have been in the headlines lately, it is not indicative of the actual picture of cyber crime.

Ostertag ascribes this decrease to wider use of encryption and the arrest and conviction of several key members of the fairly limited community responsible for the large data breaches.

While external attacks still outweigh insider attacks, insider attacks are up, especially with regard to stolen intellectual property.

The report points out that 85% of insider and privilege-abuse attacks used the corporate LAN, and 22% took advantage of physical access.

Building a bigger picture of cyber security

Now in its seventh year of publication, the 2014 data breach report analyses more than 1,300 confirmed data breaches as well as more than 63,000 reported security incidents.

For the first time, the report includes security incidents that did not result in breaches to gain a better understanding of the cyber security landscape.

Over the entire 10-year range of this study, the tally of data breaches now exceeds 3,800. Verizon is among 50 organisations from around the world that contributed data and analysis to the latest report.

“This year’s report offers unparalleled perspective into the world of cyber crime, based on big data analysis,” said Eddie Schwartz, vice-president of global cyber security at Verizon Enterprise Solutions.

“The 2014 DBIR will advance how we approach cyber threats as an industry and through our intelligence-gathering enable enterprise organisations to more strategically determine their best defence,” he said.