BIZCOMMUNITY

Tallying the real cost of a cyber attack

By Doros Hadjizenonos

24 Jan 2017

The cost of any type of theft is often a lot higher than just the value of the stolen goods. If your house was broken into, you would feel violated. While your insurance company would reimburse you for the items stolen, you might not have the same sense of security as you did before the break-in.

©Rancz Andrei via 123RF

To feel more secure, you might invest in security system upgrades and even change your habits, like going out less often or not coming home in the dark. At the end of the day, you end up spending more – and not necessarily just money – in order to feel safe again.

Corporate breaches are no different and the ripple effects of cybercrime are often more damaging than the actual theft of information. The loss of confidence – both from your company and your customers – make you overspend on security solutions, feel obligated to pay impacted suppliers and cause your customers to flee.

Initial costs

According to the Ponemon Institute, the average cost of a data breach is $154 (R2,180) per record. With many incidents involving thousands or even millions of records, the average cost of a single breach is often in the region of $3.79 million.

The initial “splash” costs of a breach – when the stone first hits the water – includes several direct expenses:

- The value of stolen intellectual property
- Downtime analysing, repairing and refortifying all compromised systems
- Checking all systems for additional infections
- Restoring systems from backups and checking backups for vulnerabilities
- Changing security procedures and training personnel on new safeguards

Ripple costs

The less obvious “ripple” costs, however, can quickly overshadow these direct costs, and include:

- **Reputational damage:** Brand value decreases 21% as a direct result of a security breach.
- **Loss of business resulting from breach of trust:** Research found that 73% of US customers switch their financial service provider due to personal data theft, and 44% of financial services companies reported business loss of 20% or more due to reputation issues.
- **Knock-on attacks:** People often use the same passwords to access different websites. Stolen passwords from one site are used in multiple breaches targeting other sites.
- **Disruption caused to other businesses, such as suppliers and partners:** In the case of critical infrastructure, if one grid goes offline, hundreds or thousands of businesses could be impacted in ways not easily quantified.

In 2013, US retail chain Target suffered a data loss event in which 40 million debit and credit card records were stolen. Direct expenses added up to $248 million over two years but some sources estimate costs will exceed $2.2 billion when including losses from fraudulent charges, reimbursing suppliers, and penalties from class action lawsuits.

The ripple effects to company reputation are difficult to estimate, but very real. If a company has strong customer support and handles the situation carefully, customers may be shaken but not leave.

Holistic security approach

Organisations can protect themselves by taking a holistic approach to security instead of patching together point solutions, and by focusing on threat prevention as opposed to threat detection and remediation. To further reduce risk, they should include data loss prevention in the security mix and use best practices when configuring security.

When considering their cybersecurity goals, organisations should ask the following questions:

- **Understand the situation:** How confident are we that our cybersecurity is effective against zero-day threats? How well trained are my employees about cyber threats and the potential consequences of their actions?
- **See what’s coming:** Do we have clear visibility of log activity in all of our network segments?
- **Secure workloads not servers:** Do the workloads I run in virtual, cloud and software-defined environments receive the same protections as workloads run in my data centre?
- **Get prepared:** Do the company’s policies protect information and resources in all environments? How is the executive leadership informed about the current threat level and potential business impact of cyber-attacks?

The volume of attacks and attack points requires complete visibility into operations and centralised security management, but not complete transparency. Security officers should be cautious about exposing protection methods or discussing attack details because when cybercriminals see where attacks have an impact, they adapt their tactics. Because of this, organisations – especially financial institutions – now share attack information through shared threat intelligence feeds.

Since most hackers use the same successful attack methods against multiple victims, it increases their costs if a hack method only works once. The more expensive hacking is, the lower the number of hackers, making everyone safer.

ABOUT DOROS HADJIZENONOS

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet
- Local eateries going digital now at risk of cybercrime - 24 Aug 2020
- How to have strong cyber hygiene - 26 May 2020
- How to approach data breaches - 11 May 2020
- Employees must be educated about mobile cyber threats - 13 Feb 2020
- Stay ahead of emerging cyber threats - 8 Jul 2019

View my profile and articles...