INFORMATION TECHNOLOGY

2010 SECURITY REPORT FROM VERIZON REVEALS NEW PATTERNS OF CYBERCRIME

(As published in *Hospitalitas*, April 2011, Issue 2)

by Kelly L. Frey, Sr.*

Each year Verizon's RISK Team produces a report analyzing data and security breaches. The 2010 study, conducted in association with the US Secret Service, analyzed 900 breaches and over 900 million compromised records and outlines some simple steps businesses can take to maintain the security of their digital systems.

Surprisingly, the Verizon report concludes that an increasing number of breaches originate from sources internal to breached organizations – mostly lower-level employees with deliberate and malicious intentions. That said, the report confirms that the largest number of compromised data records still arise from outsider attacks.

The report concludes that hacking and malware make up the most widely used attack strategy. The term "hacking" includes attempts to intentionally access or harm information assets without authorization. "Malware", on the other hand, involves software or code developed specifically for the purpose of compromising or harming information assets. Hacking most frequently involves stealing credentials (either to gain access to personally identifiable information such as financial records or access to other features of the hacked system) and can be automated or accelerated using well-known tools. Web applications seem to be the most popular attack pathway for hacking actions and were responsible for nearly all the records reported compromised. Other recent reports indicate that both hacking and malware attacks may now be expanding to mobile devices as these become more pervasive and have increase applications designed to support financial transactions and online commerce.

The report also indicates that some of the security breaches resulted from the reduced privacy expectations and vigilance individuals now exercise when using digital systems. These types of security threats employ deception, manipulation, intimidation, and other methods to obtain information directly from victims that can be used to gain access to the victim's digital information. While the report outlined well known social attacks such as phishing, pretexting, and spoofing in the context of phone and email, it also highlighted social networking sites such as Facebook and Twitter as a potential source of personal information that a criminal can use to compromise a victim's digital information.

More sophisticated hackers are noted for targeting specific types of data (such as payment card data, social security number, and bank account numbers). These attackers generally focus on the "Big Three" industries – financial services, hospitality and retail sites – where a single breach can reveal information on thousands of customers. Financial services, in and of itself, made up 94% of all compromised records in 2009.

However, the report emphasizes that the vast majority of attacks arise from less sophisticated exploits. Of the breaches recorded by Verizon, only about 15% required advanced skills or significant customization by hackers. By make small changes, such as encrypting digitally-stored data or requiring authentication when logging onto a system, businesses can effectively deter many security attacks.

In their report, Verizon advises businesses to use industry standards, such as the new version 2 of the Payment Card Industry Data Security Standard (PCI DSS) released last fall, to protect sensitive financial information of cardholders. Verizon found that of all organizations whose financial information had been breached, more than three-quarters had failed to comply with PCI DSS standards. The report suggests that most hackers simply don't want to put forth the additional effort required against protected digital system, and they are often perfectly happy to move on to the next victim if the targeted system appears to present any significant challenge.

What can be learned from these types of reports?

1. Monitor incoming and outgoing traffic

Verizon found that over 85% of attacks could be detected based simply on evidence in server logs. Thus, implementing automatic processes to search for common hallmarks of breaches in these logs can significantly reduce the risks and damages from a security incident.

2. Facilitate early warning of breaches

Data breaches are often reported not by the targets of the attack but by third-party fraud-monitoring services and the eventual victims of the data theft. So regularly monitoring public information about breaches and having a fraud-reporting number or contact within your company can facilitate early knowledge of data security compromises (and allow companies to minimize the impact of on-going attacks).

3. Restrict and monitor internal access

The report recommends limiting privileges to those who absolutely need access to data and separating duties wherever necessary to limit the amount of damage any one internal user can inflict. Logging user activity and flagging for certain types of misuse and "minor" policy violations often provide reasonable indicators of future breach.

4. Be wary of outsiders

Finally, simple restrictions like blacklisting of suspect IP addresses/websites and restricting administrative connections from outside sources can reduce a company's exposure.

In general, preventing data breaches is just a matter of common sense and following well-established security controls. Companies need to be proactive in monitoring tell-tale signs of attacks and implementing internal control processes to ensure compliance with company policies and industry standards. Last, companies need to have an easy method for reporting of security breaches and responding quickly to stop such attacks (and minimize their damage).

* Co-Authored by William K. Norton

FOR MORE INFORMATION, CONTACT:

Kelly L. Frey, is a member in Dickinson Wright's Nashville office and can be reached at 615-620-1730 or kfrey@dickinsonwright.com.