Keeping your customers' data secure in 2017

Order-ID: 16821096

Keeping your customers' data secure in 2017

What Can We Learn from the Biggest Data Breaches of the Past Decade?

According to an IBM estimate, a company's losses typically total about $4 million when a data breach occurs. That's about $158 for each customer record compromised. Even the world's largest and most technically savvy companies have not proven immune to data breaches. Some of the companies victimized in the past few years include Yahoo, Target and LinkedIn.

While it isn't possible to guarantee that your company will never suffer a data breach, it is possible to take appropriate steps to protecting your business with a liability insurance policy and learning from the breaches that have occurred. By analyzing some of the biggest data breaches of the past few years, you can learn about the weaknesses that hackers typically exploit. By minimizing or eliminating those weaknesses in your own organization, it's possible to reduce the chance of a hacker compromising your customers' data.

Yahoo Data Breaches in 2013 and 2014

In 2016, Yahoo revealed that hackers compromised the details of more than 1.5 billion user accounts in two separate attacks. In the attacks, the hackers stole personally identifiable information including names, birth dates and encrypted passwords. The hackers also stole password hints in plain text, which was information that they could have used to log in to users' accounts. Why Yahoo took so long to inform users of the attacks is unclear.

Yahoo believed that the hackers may have accomplished the attacks in part by using fake cookies, which are bits of code that a website uses to validate active login sessions, to make the Yahoo website believe that legitimate users were logged in.

Two-factor authentication is one way in which Yahoo may have been able to prevent the attacks. With two-factor authentication, a single password isn't enough to verify an account. The website also sends information to a physical device that only the user possesses, such as a mobile phone, and requires the user to enter that information to complete the login process. Two-factor authentication is inconvenient for users, but many financial and medical institutions are now requiring it for the maximum possible user data safety.

LinkedIn Data Breach in 2012

In 2012, hackers from Russia breached the professional social network LinkedIn and stole the encrypted passwords of millions of user accounts. At first, LinkedIn believed that the hackers compromised about 6.5 million accounts. LinkedIn didn't discover until 2016 that the hackers had actually compromised 167 million accounts.

Although it is unclear how the hackers managed to penetrate LinkedIn's user database, the damage from the attack was significant because the hackers were able to decipher the stolen passwords and offer them for sale. Hackers deciphered the passwords because LinkedIn used a weak form of encryption to protect them. LinkedIn stored the passwords as mathematical values called checksums obtained during the encryption process. Knowing a checksum makes it possible to test random passwords on a very fast computer without access to a server. The hackers deciphered the passwords in about one day.

LinkedIn could have prevented its users' passwords from leaking, or at least made cracking the passwords significantly more difficult, by salting the passwords as part of its encryption procedure. In cryptography, salting adds random characters to a password before encrypting it. The random data makes the encrypted password significantly longer, and the longer an encrypted password is, the more difficult brute force decryption becomes. Since the hashed password contains random characters, guessing it with words from a dictionary is impossible. LinkedIn now salts its passwords.

Target Data Breach in 2013

During the height of the 2013 holiday shopping season, hackers compromised Target's internal network and planted malware on the company's point-of-sale machines. The malware scanned the memory of the POS systems and allowed the hackers to steal about 40 million credit and debit card numbers. Some consumers reported that their cards were used to make unauthorized purchases. Banks scrambled to cancel the compromised accounts and issue new cards to their customers. Target's settlements with Visa, banks and consumers totaled more than $100 million.

Target never revealed exactly how the hackers managed to penetrate its network. However, security experts believe that they probably did so by planting malware on a computer belonging to a third-party company that serviced Target's air conditioning systems. The hackers most likely used the malware to steal the login information that the company used to access Target's network. Through Target's third-party vendor portal, the hackers somehow managed to gain escalated network privileges and plant the malware on Target's POS systems.

The Target data breach was a coordinated and well-researched attack. No single point of weakness left Target's systems vulnerable to intrusion. In fact, one report alleges that Target's intrusion detection system identified the malware and that Target didn't react to the warning. It is possible that Target could have prevented the data breach by simply not ignoring its security system.

The Target breach also serves as a warning that your company needs to exercise care when granting network access to outside vendors. With better security practices, it would not have been possible for an attacker to breach the core of Target's internal network through a vendor portal. Target also could have used two-factor authentication for its vendor portal to prevent a hacker from accessing the portal with a password alone.

If your company has terminals that need to run only a few different software applications, an application whitelisting policy can make it virtually impossible for malware to infect your terminals. Target has employed a whitelisting policy for its POS systems following the data breach. A system with a whitelisting policy refuses to run any application not specifically approved by your company's IT department. Since malware isn't on the whitelist, an infected computer can't execute it, and it has no effect.