cybereason

You Will be Breached

Critical Realizations in a Post-Breach Era

1. Even the most protected organizations will get hacked

Recent data breaches have shown that any company in any industry is susceptible to a data breach. Target, Sony, Home Depot and Anthem are just some of the companies that dedicated attackers have infiltrated. These breaches occurred even though these organizations took steps to protect themselves from cyber threats. Security professionals are starting to realize that even the most robust security measures will eventually succumb to a determined adversary. In other words, breaches are inevitable and, in fact, hackers may have already infiltrated an enterprise's network.

> *No matter how well an organization defended itself, there were always vulnerabilities a hacker could exploit.*

2. Attackers have 100 percent success rate in penetrating networks

Lior Div, CEO of Cybereason, likes to share a striking anecdote from his time as a cyber-security researcher in the Israeli Defense Forces, where some of his duties included tracking adversarial hacking teams. The teams he tracked had a 100 percent success rate when it came to network penetration. No matter how well an organization defended itself, there were always vulnerabilities a hacker could exploit.

3. The JP Morgan breach example: there is no magic shield

When the news of the JP Morgan breach became public, it was revealed that the hackers were able to access JP Morgan's internal server because two-factor authentication was not enabled. Although two-factor authentication could have prevented hackers from utilizing that breach method, it would have ultimately failed to stop hackers from penetrating the network.

The JP Morgan internal breach was possible because attackers obtained a private certificate from, Simmco Data Systems, the vendor that created

websites for the financial services company. With this certificate, attackers were able to hack 420,000 websites, created by Simmco, including the site for the JP Morgan Corporate Challenge.

The Corporate Challenge website hack wouldn't have given hackers access to JP Morgan's internal site. However, many of company's employees used their JP Morgan log-in credentials to access the Corporate Challenge site, which provides information on a series of road races put on by JP Morgan. Armed with this information, the hackers easily and successfully accessed JP Morgan's network.

Even if JP Morgan had used two-factor authentication to thwart the hackers, they would have undoubtedly tried other methods until the attack was successful.

For example, the hackers already had the log-in credentials of JP Morgan workers who accessed the Corporate Challenge website along with information about what races they ran. Attackers could have used these personal details to craft a spear-phishing email about an employee's participation in the race. When a highly customized email that references a specific events, like a road race, arrives in an inbox, a worker could mistake it for a legitimate correspondence, open it and download the malicious content that's attached. Remember, only one employee needs to fall.

The media debate claiming that the **JPMorgan breach could have been prevented** by **proper implementation of two-factor authentication** clearly demonstrates that the public is still searching for a magic shield that can prevent hackers from successfully penetrating a corporate network.

In reality, however, there is no unbreakable system. Professional cyber criminals have the time and the financial means to deploy many different methods until they break the defender's shield.

4. Post-penetration: security has time to act

After infiltrating a network, cyber criminals slowly inflict damage. They gradually move around a network and perform minimal daily actions to avoid detection. This gives security teams an opportunity to detect the breach early, reducing its scope and cost.

In JP Morgan's case, it took between two and four months for the breach to be discovered. This delay gave hackers more time to collect their bounty: information on 83 million user accounts and high-level access to 90 servers.

Even if the initial penetration was impossible to detect, many of these hackers' activities could have been identified. For instance, closely monitoring the IT environment would have revealed anomalies while linking together seemingly benign events could have formed a clear picture of malicious activity.

> *Accepting that a network breach is inevitable requires security teams to adopt a new post-breach mentality.*

Developing post-breach capabilities is crucial

Accepting that a network breach is inevitable requires security teams to adopt a new post-breach mentality. Part of this mindset entails improving network and endpoint visibility so organizations can better identify irregularities and malicious activity. Since a hacker's activity on a network only deviates slightly from typical user behavior, an organization needs to continuously monitor behaviors and to see minor changes.

The post-breach mentality also incorporates situational awareness into a security plan. Obtaining that insight requires collecting and analyzing gigantic amounts of data in real time. To better carry out these big-data projects, the post-breach mentality requires using machine learning to automatically figure out a company's IT environment and use context to distinguish between normal and unusual behavior.

Imagine the most innovative automated video analytics technologies that the U.S. Department of Homeland Security deploys in airport to detect possible threats. These technologies analyze video streams of security lines in real time, learn common behaviors and flag abnormal activity. Next, facial recognition technologies are used to identify suspected terrorists and issue alerts on individuals with high security significance. A similar approach should be used by enterprises to help them fight complex hacking operations.

cybereason

Cybereason was founded in 2012 by a team of ex-military cybersecurity experts to revolutionize detection and response to cyber attacks. The Cybereason Malop Hunting Engine identifies signature and non-signature based attacks using big data, behavioral analytics, and machine learning. The Incident Response console provides security teams with an at-your-fingertip view of the complete attack story, including the attack's timeline, root cause, adversarial activity and tools, inbound and outbound communication used by the hackers, as well as affected endpoints and users. This eliminates the need for manual investigation and radically reduces response time for security teams. The platform is available as an on premise solution or a cloud-based service. Cybereason is privately held and headquartered in Boston, MA with offices in Tel Aviv, Israel.