channel insider

The Real Cost of Security Attacks to U.S. Business

One of today’s main business challenges is the gross number of ever-increasing security threats.

According to Ponemon Institute researchers, the average total cost of a data breach throughout the world grew from $3.8 million to $4 million over a 10-month period. In addition to cost, the global study puts the likelihood of a material data breach involving 10,000 lost or stolen records in the next 24 months as high as 26 percent.

Yet, amazingly, many companies still are not taking security seriously enough. Taking a reactive approach will no longer work, as a threat may already be causing massive damage by the time it’s identified.

Distributed denial-of-service (DDoS) attacks, which overload a server with traffic to push it offline, are steadily increasing, and we have also seen a massive rise in new threats such as “DNS tunneling,” in which the Domain Name System protocol is used to maliciously steal data. “DNS water torture” is another tactic (also known as a “Slow Drip DDoS attack”), which makes a victim’s domains appear inaccessible.

Research From EfficientIP

The repercussions of these breaches aren’t just short-term monetary issues due to application downtime. They can also include long-term loss of business due to permanent brand damage. EfficientIP recently spoke with nearly 1,000 participants as part of a survey we conducted this year on DNS attacks, and it was determined that 27 percent of U.S. respondents didn’t feel DNS security was critical to their businesses–a vast majority weren’t even aware of the different types of vulnerabilities.

We then looked at the state of DNS security in U.S. organizations and just how much damage is being done.

How susceptible are U.S. organizations to DNS attacks?

Of the U.S. respondents to EfficientIP’s survey, as many as 31 percent were involved in vicious volumetric attacks (DDoS or DNS amplification); further, 10 percent were involved in zero-day vulnerabilities. An additional 14 percent of respondents were subject to DNS-based malware attacks.

This certainly points to U.S. companies being susceptible to DNS attacks, and as a result, they are losing considerable sums of money.

Are effective measures being deployed to mitigate DNS attacks in the U.S.?

As many as 25 percent of respondents had to shut down their servers. Further, 19 percent closed down specific affected processes and connections, and 39 percent needed six hours or more to mitigate an attack. This is a lot of wasted time–applications are down, people are not able to do their jobs. These companies are risking both short- and long-term damage to business by inadequate and reactive DNS security measures.

What’s the extent of the damage to U.S. business?

Reactive measures to security threats, such as shutting down servers, are causing damage to business availability and reputation. Almost 16 percent of respondents to EfficientIP’s study have experienced loss of business from an attack, and almost 13 percent have suffered brand damage. Further, 25 percent have had their websites compromised, and as high as 43 percent have been impacted by application downtime.

What’s next for U.S. enterprises and their IT departments?

The reality is that DNS attacks are becoming increasingly sophisticated, and are only going to cost businesses more. Recent news stories featuring high-profile cyber-attacks highlight the importance of cyber-security. These stories include the recent four-day-long DDoS attack on the Library of Congress, which caused intermittent outages of service for websites and agencies under the library’s umbrella, including the U.S. Copyright Office; as well as the attack on Pokémon Go servers this summer by the hacking group PoodleCorp, which claimed responsibility.

Attacks of these proportions are occurring with increasing frequency, and these two examples are just a small fraction of the cyber-attacks that are occurring daily. Although many organizations are beginning to take notice, those that are not (or are not fully prepared) are at risk of permanent loss of data, and more importantly, their business.

For this reason, it is critical to stay ahead of threats by using security solutions and systems that can protect against an increasingly large and complex range of attacks. A consistent, unified and streamlined process is required to meet the needs of the constantly changing security environment.

There are many dependable solutions available that offer high availability, and ensure no impact on business activity alongside a highly secure network. These solutions guarantee reliability, scalability and flexibility, while also speeding up deployment, reducing costs and increasing productivity. This should be of particular interest to the channel due to the many aspects of deployment and continued involvement with customers.

U.S. companies can't afford to lose any more of their customer data or intellectual property. A staggering 8 percent of U.S. respondents to the EfficientIP study experienced DNS tunneling and data loss in the past year. This translated into almost 13 percent of businesses incurring more than $1 million in damages (a mission-critical growing market segment that could provide channel opportunities). Don't let it be you or your customers.

David Williamson is the CEO of EfficientIP, a DDI provider headquartered in Europe, Asia and North America. (DDI refers to three network services: Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) and IP address management (IPAM).)