WatchGuard's 2012 Security Predictions

2011 proved to be a memorable year for information security. The security analysts at WatchGuard cannot remember a year with such newsworthy security incidents and discoveries as 2011 delivered. With disastrous breaches, like those suffered by Epsilon, RSA, and Sony, to amazingly advanced malware, like TDL-4 and Duqu, 2011 was an unforgettable year for security practitioners - one that we hope to never see the likes of again.

As has been the tradition for the past 15 years, WatchGuard once again provides a peek into the future of network and information security with the top 10 areas of concern for 2012. In this year's predictions, some are new and some are a carryover from 2011. No matter though, they are all very serious.

A Cloud Provider Will Suffer a Significant Security Breach

Cloud computing brings chance of malware storms

In 2012, expect organized criminals to target cloud services, and significantly breach at least one well-known cloud provider. That said, expect to see smarter, trustworthy cloud providers recognize that risk and add premium security to their offerings.

Over the past few years, the IT industry has been abuzz over cloud computing. Consensus among IT circles holds that everything will move to "The Cloud," thus saving time and money, and simplifying our lives. Whether this is true or not, one thing is certain - attackers have noticed this trend and will take advantage of it.

While many cloud services offer attractive benefits, they also leverage complex technologies that have security ramifications. Most cloud providers rely on intricate, custom-made web applications, or leverage virtualization to provide scalability and multi-tenancy. While these are great technologies, they can also pose dire risks when implemented incorrectly, causing systems to no longer be secure. Add to the equation the fact that many customers share sensitive data with one popular cloud provider. It is easy to see why a single large cloud provider presents a juicy target to attackers.

Organized Criminals Will Leverage Advanced Malware Techniques in Targeted Attacks against Businesses

Advanced Persistent Threats (APT) trickle down to SMBs and Consumers

Expect the APT trend to continue in 2012, but with a slightly new twist. APTs will trickle down to everyday people.

Last year, we told you to expect to hear more about advanced persistent threats (APT), and to expect to see more real-world examples. This prediction seems to have proven true with large breaches like RSA's SecureID incident and operation ShadyRat, as well as the discovery of Stuxnet's successor, Duqu. As expected, these APTs of 2011 primarily affected very big organizations, such as governments, industrial control providers, and large enterprises.

In 2012, less sophisticated criminals will start to leverage the advanced techniques they've learned about from APTs to create more advanced malware that targets smaller businesses as well as consumers.

The Barrage of Noteworthy Data Breaches Continues through 2012

Hacktivists and script-kiddies rage against the machine

One prediction WatchGuard wishes it had made for 2011 was that it would be the year of big breaches. Whether due to APT attackers, criminal malware authors, or hacktivist groups like Anonymous and LulzSec, we witnessed more headline-grabbing hacks than we ever remember seeing before.

It's hard to say if the increase in reported breaches is due to smarter criminals, more attacks, hacktivists, or just new regulations that require businesses to inform us when they lose data. In any case, expect this trend to continue in 2012. Now that criminals realize how much they can profit by stealing data, and hacktivists realize that network attacks draw attention, we suspect they'll both continue besieging networks next year.

Increased Reliance on Virtualization Reawakens Need for Virtual Security

Unprotected virtual machines make bad neighbors

Expect to see a considerable rise in interest for virtualization security solutions among smaller and midsize businesses next year due to their increased reliance on this technology.

Virtualization is no longer the new technology on the block. Enterprises have leveraged it in production environments for years; most IT professionals have become familiar with it, and have at least experimented with it as a tool. In short, virtualization has begun to mature.

So what's new and how does this affect security? As with other emerging technologies, as virtualization matures, its usage increases among smaller companies and organizations. Many small and midsize business IT professionals still don't grasp the potential security ramifications of poorly implemented virtual environments. Because of the lack of security know-how and increased reliance on virtualization, risk of data loss dramatically increases.

Smartphone App Stores and Marketplaces Help Proliferate Mobile Malware in the Real World

Unprotected virtual machines make bad neighbors

In 2012, WatchGuard forecast the mobile threat will continue to grow, but with a more specific source- app stores and marketplaces. To avoid mobile malware, be careful of what is downloaded from an app marketplace, and hope the associated vendor does a thorough job validating apps.

In the past, we've predicted attackers will increasingly target mobile devices, like smartphones. After all, smartphones and other mobile devices are just small computers, and thus, suffer from all the same security issues as their larger counterparts. Though the growth of mobile malware has been gradual, this prediction has proven to be a yearly trend, with AV companies seeing annual increases in smartphone malware.

During 2011, attackers primarily focused their malware delivery efforts on infecting various smartphone providers' application delivery system, like Google's App Marketplace or Apple's App Store. They've been more successful at infecting some app stores than others, but have demonstrated that all application repositories can be fallible.

Adoption of BYOD and IT Self-Service Results in More Data Loss

Bring your own device means clean your own infections

In 2012, WatchGuard anticipates several data loss incidents and breaches as a result of the increased adoption of Bring Your Own Device (BYOD) and self-serve IT. This isn't to say organizations can't implement these concepts securely, only that they are such new concepts that few really know how.

BYOD is becoming a fad among trendy IT departments. On the surface, it seems to make sense. They say it can reduce IT costs, increase productivity, lessen helpdesk load, and just plain make employees happy. After all, employees are already secretly using their own devices anyway, right?

Employees aren't only bringing their own devices, but launching their own network services. New cloud offerings make it possible for non-IT departments to easily contract and launch new technical services, without the help of their IT department. Industry pundits call this trend the "consumerization of IT."

While BYOD and IT self-service do offer some clear benefits, they also come at a price; the potential loss of control. Offloading your IT services and device purchase decisions to others makes it infinitely harder to implement access controls on those services and devices.

As the Top Vector for Social Engineering and Malware, Facebook Is Forced to Increase Its Security

If Facebook doesn't "like" security they'll surely get "poked"

Two years ago, WatchGuard predicted social networks would be a dangerous playground for attackers. Last year, we predicted that Facebook links would take over where malicious email attachments left off. This year, both those predictions continue to prove true. Expect to see more Facebook security updates next year.

In fact, in 2012, we forecast Facebook-based attacks will increase and Facebook will be forced to sit up and take notice. Specifically, Facebook will implement new security solutions on their site to avoid losing disgruntled users. This has already begun as Facebook has partnered with WebSense for URL scanning.

Attackers Launch a Digital Attack that Affects Physical Infrastructure or Equipment

My power plant got a virus infection

Expect at least one digital attack in 2012 that causes a significant repercussion to a physical system.

Information security professionals have always imagined scenarios where digital attacks would have actual physical repercussions or do damage in the real-world. Though these sorts of attacks have long been theoretically possible, we had never really seen one happen until Stuxnet came along. Stuxnet actually infected SCADA equipment, and made changes that had real physical results.

Since then, researchers and attackers alike have heavily targeted SCADA systems. Now that they've seen what highly advanced malware can accomplish against industrial control systems, they've gone all in.

Location-Aware Malware Customizes Its Attacks

Spyware knows where you live

Geolocation is a hot topic among security experts, simply from the standpoint as a potential privacy violation. Privacy advocates don't like that legitimate software might know where individuals are, since they imagine big brother and big business leverage this information to track personal habits. Don't like the idea of your iPhone keeping tabs on you? Imagine how you might feel if malware leveraged geolocation for even more nefarious purposes.

That's exactly what we suspect will happen in 2012. Malware will increasingly leverage geolocation to customize attacks, thus increasing its money-making potential. A simple technique already in use is to forward victims in specific locales to targeted fraud sites that work best in that region. We anticipate hackers will find more malicious ways to exploit geolocation in malware next year.

HTML5 Offers Five Times the Ways to Hijack Your Website

New web technologies like HTML5 fuel the growth for next year's web application attacks

WatchGuard predicted long ago that the web is the battleground for Internet attacks. This has proven true over the years, with web application attacks leading the "network attack" charge, allowing bad guys to steal terabytes of data in 2011.

The use of Web 2.0 and other dynamic web technologies is one of the key contributors to attackers targeting the web. These immensely powerful and useful web technologies are not inherently insecure. In fact, they fuel just about every major web site on the Internet, including some of the largest cloud-based web applications that drive businesses today. However, if web developers don't follow secure coding practices, the same powerful web applications that drive business, could allow hackers to crash right into corporate networks.

Like the web technologies that preceded it, HTML5 is not inherently insecure. In fact, it actually introduces some security benefits that could help smart developers avoid some web application pitfalls. However, the security of HTML5 applications is still dependent on the skill and care with which developers create them. HTML5 is new and complex. Developers are still getting comfortable with it, which means they are likely to make programming mistakes that could translate into web vulnerabilities. For this reason, we predict that the increased usage of HTML5 will significantly contribute to the continued increase in web applications attacks next year.

Conclusion

Last year reminded us that discovery and response are as crucial to network security as prevention and maintenance. We suggest spending as much effort in the coming year rooting out potential breaches as time spent trying to prevent them. In both cases, WatchGuard stands committed with tools and solutions to help.

WatchGuard Technologies provides an extensive family of network security products to help you secure your network from advanced attacks, stop sensitive data from leaving the network, block social networking sites, prevent malicious intrusions, integrate in-the-cloud security services, and much more – all with unprecedented visibility into network security activity. For more information, contact your reseller or visit us at **www.watchguard.com**.