TRENDING The science behind why humans prefer printed books

Future Trends /

10 massive online security predictions for 2016

By Doros Hadjizenonos on 6 November, 2015

3 15

A year in cybersecurity can seem like an eternity. But despite the rapid changes, many things remain constant. Check Point's top three predicted security threats for 2015 were the rapid growth in unknown malware, in mobile threats, and in critical vulnerabilities in commonly used platforms (Android, iOS and others). These were fully realised, and are likely to remain a significant threat. The cat-and-mouse game that has typified cybersecurity in recent years continues, with hackers constantly finding new ways in which to attack networks – as this year's high-profile breaches at Anthem, Experian, Carphone Warehouse, Ashley Madison and TalkTalk showed.

Like most IT security professionals, I really want my predictions not to come true: I would prefer organisations didn't get hacked or breached. But by anticipating the next wave of threats, we hope to help businesses stay on top of the evolving tactics and exploits that criminals will use to target them. So here are ten IT security threats and trends that I expect we will see during 2016.

1. 'Sniper' and 'shotgun' malware

We believe that larger breaches in 2016 will be the result of custom-designed malware designed to get past the defences of specific organisations, such as the attack on US retailer Target. While generic, broad-brush attacks will continue to threaten individual users and small enterprises, hackers will raise their game when attacking larger organisations with more sophisticated security postures. They will use deeper, more sophisticated phishing and other social engineering tricks to gain access to the data that they want.

2. Moving to mobile

Mobile attacks continue to increase as mobile devices become more commonplace in the workplace, offering hackers direct and potentially lucrative access to personal and corporate data. Our 2015 Security Report found that 42% of organisations had suffered mobile security incidents which cost more than US$250 000 to remediate, and 82% expected incidents to rise. This year has also seen several high-profile mobile vulnerabilities emerge, including Certifigate on hundreds of millions of Android devices and XcodeGhost, the first major malware infection targeting non-jailbroken iOS devices. We expect to find more major mobile vulnerabilities in the next year.

3. Threat prevention

In the ongoing battle between hackers and security professionals, attackers are increasingly deploying more sophisticated, custom variants of existing malware and zero-days that can bypass traditional sandboxing technology. These new attack vectors require more proactive and advanced solutions that catch evasive malware. CPU-level sandboxing is able to identify the most dangerous threats in their infancy before they can evade detection and infect networks.

4. Attacks on critical infrastructure

In December 2014, a steel mill in Germany was hit by hackers who accessed the plant's production network and caused 'massive' damage. Also, the US Department of Homeland Security that 'Havex' Trojan infections had compromised industrial control systems in over 1 000 energy companies across Europe and North America. Attacks on public utilities and key industrial processes will continue, using malware to target the SCADA systems that control those processes. And as control systems become increasingly connected, this will extend the potential attack surface – which will require better protection.

5. IoT and smart devices

The Internet of Things is still emerging and is unlikely to make a big impact in 2016. Nevertheless organisations need to think about how they can protect smart devices and prepare themselves for wider adoption of the IoT. The key questions users need to ask is 'where is my data going?' and 'what would happen if someone gets hold of this data?' A year ago, we discovered a flaw in SOHO routers worldwide that could allow hackers to hijack the router to launch attacks on any devices connected to it – and we will see more of these vulnerabilities in connected devices.

6. You wear it well

Wearables like smartwatches are making their way into the enterprise, bringing with them new security risks and challenges. There are a number of security concerns about data that is held on smartwatches, or that wearables could even be used by hackers to capture video and audio via mobile remote access Trojans, so organisations that permit these devices need to ensure that they are protected with encryption and strong passwords.

7. Trains, planes and automobiles

2015 saw the emergence of car hacking, in which the vehicle's software is hijacked to take control of it. In July, Fiat Chrysler recalled 1.4 million Jeep Cherokee vehicles in the US after security researchers found that they could be hacked via the connected entertainment system. With modern cars featuring more gadgetry and connected systems than ever before, we need to apply protection to these in-car systems – and the same applies to the complex systems in passenger aeroplanes, trains and other forms of public transport.

8. Real security for virtual environments

Virtualisation has been adopted rapidly in the enterprise over recent years, whether it's through SDN, NFV or cloud computing. Virtualised environments are complex and create new network layers, and it's only now that we are seeing a real understanding of how to secure these environments. As organisations move to virtualised environments, security needs to be designed in from the outset to deliver effective protection.

9. New environments, new threats

2015 has seen the launch of a number of new operating systems, such as Windows 10 and iOS 9. The bulk of enterprise attacks in recent years have been on Windows 7, since adoption of Windows 8 was relatively low, but with Windows 10 experiencing a high uptake driven by the free download available, cyber-criminals will turn their attention to trying to exploit these new operating systems where updates are more frequent and users are less familiar with the environment.

10. Security consolidation – keep it simple!

To protect against multifaceted threats, security professionals are likely to increase their reliance on centralised security management solutions. With large enterprises having a plethora of different security products on their network, consolidation offers a way of reducing both complexity and cost. Having many point products and solutions quickly becomes unmanageable and can actually impede, rather than improve security, so consolidating security provides an effective way to cut complexity and make for easier management, so that new threats don't get lost in the gaps between systems.

RELATED

- What's next? 6 top trends for the BI industry in 2016
- The satellite internet landscape in Africa – developments and future scenarios
- 5 jobs ripe for automation

3 15