Blind spots and security basics – letting your guard down could cost you in 2017

Fujitsu Security Operations Centre Threat Predictions Report

shaping tomorrow with you

FUJITSU

Contents

Introduction

» In the world of cyber security, looking back is just as important as looking forward. We need to examine the learnings of the past to prepare ourselves for the threats of the future.

As such, this report will look back at our predictions for 2016 and how well they fitted into the actual events, as well as giving our thoughts on what lies ahead in 2017.

I hope that this report provides your organisation with not only a handy retrospective, but also a glimpse of what is to come so you can keep your business protected.«

Rob Norris
Head of Enterprise Cyber Security, EMEIA

How accurate were our predictions for 2016?

We predicted that there would be an increased number of serious DDoS attacks as a result of the continued growth of the Internet of Things (IoT). Some major organisations were impacted during 2016 by DDoS attacks from an IoT botnet, comprising of DVRs and CCTV cameras. The attacks affected DynDNS, which disrupted online services to Spotify, Twitter, GitHub and PayPal amongst others in October. KrebsOnSecurity also suffered one of the largest attacks ever seen.

We also suggested that web apps would find themselves under increasing attack, and, unfortunately, many attacks continued to be successful with Russian social media firm VK and the Qatar National Bank compromised by SQL injection attacks early in 2016.

Attackers continued to target data that was valuable to organisations. Universities and legal firms were big targets for attackers in 2016 with theft of data or ransomware being two primary tactics. The University of Calgary admitted it paid $20k to decrypt files impacted by ransomware.

We predicted biometrics would be on the rise. Fujitsu continues to develop some of the world's leading technologies in biometrics and many vendors are now looking to enhance their hardware solutions. Whilst Apple has had fingerprint biometrics in its iPhone for some time, it finally added biometrics to its Macbooks in 2016 shortly after NIST announced it would no longer support SMS as a secondary method of two-factor authentication.

We said Flash would be in the spotlight as it continued to be a target for attackers via exploit kits. The major browsers removed Flash as a default option whilst YouTube moved to HTML5 by default so we were correct in our assumptions about this application.

In addition, we correctly predicted that personal information would become increasingly tied up with cyber attacks. The UK National Lottery was one such victim of these attacks. 26,500 player accounts were hacked, compromising information such as dates of birth and card details.

We are confident that companies will need to be vigilant for further cyber security challenges in 2017. Our top 10 predictions are outlined over the following pages.

Fujitsu's Top 10 Cyber Security Predictions for 2017

1

Many companies will continue to have a blind spot

We predict attacks will continue to be successful in 2017 as organisations still don't address the blind spot that exists with attacks over encrypted channels being missed due to the lack of SSL inspection capabilities. 2016 also saw a huge rise in attacks against enterprises using Microsoft PowerShell. PowerShell is a framework and scripting language that is installed by default on all Windows computers and attackers are using it as many organisations lack adequate protection for malicious use. As it's already part of the Windows system, it is easier for an attacker to use it as part of their attack cycle and difficult for network defenders to identify malicious use, if they're monitoring at all. Tools such as PowerShell Empire, frequently used by penetration test teams, are also used by attackers to make it easy to bypass the perimeter, create backdoors and then move laterally around a network. Organisations will need to review their monitoring capabilities, logging levels and also work to identify what known good scripts are in use across their networks to have the ability to detect malicious attacks where possible.

2

Artificial intelligence will change analysis in security operations centres (SOCs)

As organisations seek to use artificial intelligence (AI) and machine learning capabilities, the way organisations analyse security events will change in 2017. The principle of 'what good looks like' in cyber security terms has been around for a long time. Machine learning is an extension to this concept with algorithms of what good behaviour is deemed to be, such as how certain system calls should or shouldn't be made or how certain file types are put together, so any deviation from this should be deemed suspicious. Core network monitoring for anomalous behaviour such as large transactions or first attempts to access a database will be a change in approach for security operations centres, who need to move towards an intelligence-led approach. They will no longer be reacting and triaging 'known bad' traffic via an antivirus or intrusion detection alert but will need to investigate an alert advising them something unusual has happened based on a machine learning algorithm. One further area to watch out for in 2017 is attackers using the same AI capabilities as they seek to defeat network and security controls.

3 Criminals will continue to target core banking applications

Core banking applications saw themselves become a target in 2016. Major compromises at international banking institutes saw millions of dollars stolen directly as a result of weaknesses in the SWIFT global payment network. The largest case being $81 million dollars from a Bangladeshi bank. We also observed the growth of banking Trojans targeting 'back office' applications for criminals to exploit legacy technologies to steal financial rewards directly from banks. We consider this a significant risk to the banking sector in 2017. SWIFT has introduced 16 mandatory controls and will inspect banks in 2018 for conformance but this still presents a window of opportunity for cyber criminals. Researchers identified the Odinaff Trojan targeting SWIFT late in 2016 and we expect to see new variants and methods of attack this year.

4 Attackers will increase focus on the mobile market

Improved security on new operating systems and the increasing use of smart devices for personal and business data will make mobile platforms an increased target in 2017. Many organisations are now upgrading from legacy Microsoft operating systems that have been frequently targeted for their vulnerabilities and are taking advantage of the improved security features that come with a Windows 10 build, Edge browser and improved server operating systems. Small apps, such as Adobe Flash, whilst also frequently targeted, particularly by exploit kits, are also now being removed from enterprise networks and browser providers with Google Chrome making HTML5 the default option in December 2016. Individuals now have multiple smart devices, many of which hold vast amounts of personal and business data due to modern storage capabilities and, as such, attackers will continue to develop innovative attacks against mobile platforms with mobile ransomware demanding payment for the return or decryption of personal photos. Mobile device management will need to be supplemented by robust security controls, particularly for business devices.

Hackers will target smart cities

5

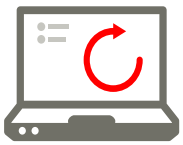
As we continue to see the exponential growth of the Internet-of-Things devices, we will continue to observe security issues that we hadn't even considered before. When an architect put together the design of smart motorway noticeboards, they didn't consider hacktivists would target them to display politically motivated messages instead of motorway warnings to motorists. The same is true of IoT manufacturers who built the hundreds of thousands of CCTV cameras, DVRs and SOHO routers that now make up the IoT 'Mirai' botnet.

Lessons will clearly be learned from Mirai, such as avoiding hard coding default passwords but many of the protocols designed for smart connected devices will have their own potential flaws and vulnerabilities as we have seen with the Zyxel routers. We will see more of these vulnerabilities in 2017.

Attackers have exploited these vulnerabilities to their advantage already so whilst ransomware having the ability to take out a city of 'smart' connected lights would have seemed unlikely and unfeasible 12 months ago, recent events have changed that perception.

It's not only the potential vulnerabilities in smart devices but these platforms also need to be controlled and the governance around the management of those control platforms will be paramount. This includes the security controls of the supply chain involved in the delivery and control of any part of the smart city we're now connecting. If it only takes a breach of one part of the supply chain to compromise the platform managing the smart devices, then we should expect to see more of these attacks. Attackers may not try to exploit vulnerabilities in connected cities but they may seek to install ransomware in a critical part of the infrastructure.

6

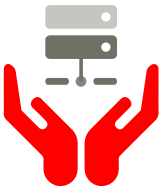


Resilience and recovery will become commercial differentiators

Cyber attacks are now so powerful that even the most secure organisations could be hit. In 2017, the question will be – how quickly can they recover?

A quick and full recovery will attract sympathy and respect from the markets, while a poor recovery will attract criticism and lawsuits. At the end of November, the San Francisco Municipal Transportation Authority suffered a major ransomware attack but, because of a robust backup process, restored most functionality within a day.

Next year, we will see which companies are serious about the challenge by whether they take a coordinated approach combining protection, detection and response.



7

Curation of data will become a key focus for all organisations, not just the data-rich

In 2017, more investors, shareholders, customers and regulators will want to see that sensitive data is being carefully looked after. This will be especially important with the approach of the General Data Protection Regulation. Specialist data loss prevention (DLP) tools work well if used properly, but many businesses either approach DLP piecemeal or assume that using a DLP tool alone is enough.

Organisations will need to look at the risks, find the key data to protect and watch their networks carefully. They will also need to protect the sensitive data of third parties as much as they protect their own.

8

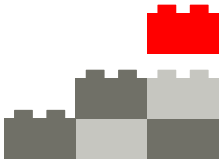
Global clients will demand to inspect their supply chains' data security

Most organisations know that their sensitive data isn't just held internally. It's also in their supply chain. However, there is often a big difference between what organisations expect of their suppliers and what suppliers contractually have to do.

As awareness of cyber security risks grow, we are starting to see global businesses look for clear proof of good data security from key professional advisers. These include law firms, accountancy practices and business consultancies. The biggest clients are well placed to insist on good data security as a condition of working with such advisers. This trend appears set to grow long into 2017 and beyond.

9 Board meetings will routinely discuss IT security

With so many cyber attacks happening against major organisations, even the most technophobic senior executives can't dismiss the issue as something to be handled purely by the IT department. 2017 will be the year that boards understand how poor IT security could hurt their businesses. Organisations will need to train senior IT staff so they can understand the board's requirements and how IT can be discussed in a language they understand.



10 Poor routine IT practices will still cause the most avoidable harm

Most of the time, the cyber-security problems that hit organisations aren't created by new cyber-attack techniques or malicious insiders. An amazing number of businesses don't carry out the simple – yet vital – housekeeping tasks that cut down on risks.

They don't have effective vulnerability patching or appropriate threat intelligence. They don't use an access management system that truly reflects only current users. They don't use 'least privilege' access or act on advice from penetration tests. This leaves them needlessly vulnerable to data loss, data theft or external disruption of their systems.

This will sadly continue into 2017, meaning most of the headlining breaches of next year will be avoidable.

Attacks will happen. Are you prepared?

2017 will see more powerful security breaches happening on a regular basis. Companies from all major business sectors across the world will be affected. This includes well-established mega-corporations, major governments and household names. Some will be unlucky. But many others will suffer attacks that could be avoided with a little more care and attention.

Please visit the Secure Thinking website to find out more about keeping your business protected, and how Fujitsu can help you to manage the ever-changing landscape of cyber security threats.

shaping tomorrow with you

FUJITSU

FUJITSU

22 Baker Street
London W1U 3BW

Tel: +44 (0) 1235 79 7711
Email: askfujitsu@uk.fujitsu.com
Web: **uk.fujitsu.com/securethinking**
Ref:3684