Cyber Security Trends 2016

Market trends from leading security analysts and consultants at TÜV Rheinland, OpenSky, and OpenSky UK

December, 2015

OPENSKY
A TÜV Rheinland Company

Cyber security Trends 2016

What do new technologies and the ever increasing cyber threat hold in store for business and the public sector in 2016? How should organizations be preparing themselves? What should IT security leaders be doing as a priority in the coming year? These are the questions we asked our leading security analysts and consultants at OpenSky to tackle.

Executive Summary

2016 will see an increasing number of attacks and the emergence of new targets. The complexity and sophistication of attacks, initiated by increasingly capable and technically well-equipped cyber criminals, will continue to rise.

In a world where 100% protection can't be achieved, every organization, no matter its size, is a target. "It is even more important, beyond taking preventive measures, for organizations to be able to maintain or restart their operations as soon as possible after an attack. That requires organizations to have established a comprehensive set of security incident response processes ahead of time" according to Olaf Siemens, Chief Executive Officer of OpenSky and Executive Vice President of the Business Stream ICT & Business Solutions at TUV Rheinland, the parent company of OpenSky.

The good news is that, after years of checkbox compliance — which doesn't keep you safe — organizations are beginning to focus the necessary resources on information security and risk management, especially as it is now firmly on the Senior Leadership's agenda. This will give IT security leaders the opportunity to consider the following trends:

1. Cybercrime becomes easier and more lucrative
2. Connected everything fuels the emergence of new attack vectors
3. The cloud forces new and emerging operating models
4. Information security goes beyond simple compliance
5. Mounting pressure for adequate data protection and data security defines public debate
6. Incident response becomes business as usual
7. Organizations increasingly need to use Managed Security Services
8. Industrial Control System (ICS) security becomes more important than ever
9. Cyber threat intelligence becomes essential for information security

1. Cybercrime becomes easier and more lucrative

Cybercrime continues to mature and become industrialized—it is becoming professional. Malware toolkits are available as cybercrime products with after sales support, and capabilities like 'Distributed Denial of Service' (DDoS) are available as volume priced cloud services. Increasingly these types of products and services can be obtained free of charge. This is an unavoidable trend which organizations can face only by acknowledging it, being proactive, and taking proportionate measures to protect themselves.

It's the continued digitization of business and the public sector that has made cybercrime increasingly lucrative and, as a result, has attracted the attention of organized crime using the latest 'Advanced Persistent Threat' (APT) techniques. Whether a large Enterprise or hidden champions of the small-medium business segment: All companies have to expect to be targeted.

2. Connected everything fuels the emergence of new attack vectors

Attacks on connected cars, connected medical devices, and connected critical infrastructure have all hit the headlines in the recent past; and this is just the tip of the iceberg. As industrial control systems become increasingly networked (Industrie 4.0), technology ecosystems—once considered secure—will become vulnerable. The creation of new connected devices and the Internet of Things is turning into a goldmine for cybercriminals. This is particularly true of the consumer devices that act as a link between the connected 'thing' and its backend systems.

Today, manufacturers still focus their attention too heavily on features, and pay insufficient attention to security. Fortunately, with the rise of cyber-related news headlines, consumers are beginning to appreciate the importance of cyber security and will demand it from the marketplace. For manufacturers to achieve this, 'secure by design' becomes a critical success factor.

However, it remains to be seen just how quickly manufacturers will 'bite the bullet' and take the initiative to provide better protection, for their connected products and services, against the threat of cyber-attack. Not only could they suffer economic losses and reputational damage, adequate cyber security will increasingly be demanded by consumers who will also be willing to pay for it. Hopefully, manufacturers will not need to suffer a major incident in order to provide the deciding impulse.

3. The cloud forces new and emerging operating models

Business and the public sector continue to transition to the Cloud, as it is generally accepted that the agility and cost benefits outweigh the perceived risks. However, moving to the Cloud does not absolve organizations of their accountability to protect their corporate and customer data. Instead it changes the operating models and forces organizations to address how they will share the responsibility with their cloud providers and manage the risk. It affects incident response structures and measures, and makes identity management and access protection the new organizational perimeter. It raises the question as to how cloud consuming organizations will continue to prevent, detect and respond to security events and then ensure these

capabilities are at the core of their cloud strategy. Part of the answer will be encryption - ensuring data is encrypted before it enters the cloud and, that the accountable organization, not the cloud provider, manages the encryption keys for themselves. Solid IT governance practices will be required to ensure that, during the transition, an organization's IT infrastructure continues to support and enable the achievement of its corporate strategies and objectives.

4. Information security moves beyond simple compliance

To be able to keep corporate and customer data safe from the professional cybercriminal, it is becoming increasingly important for organizations to move beyond the compliance mentality of focusing on security controls and vulnerabilities, and take a risk-based, treat modeling approach. A risk-based approach introduces the relationship between assets, threats, vulnerabilities and controls. This 'threat modeling' focuses on where data is generated, how it flows through systems, where it is stored, and how it is aggregated; it is particularly relevant in relation to connected medical devices and healthcare sector today.

Data governance, protection and consent models will become increasingly important to assure the integrity, confidentiality and security of corporate and customer data. Risk-based techniques applied against a clear understanding of data flow will be essential to enable business growth in a digital economy. IT risk will gain increasing emphasis on the corporate risk-register as a means to safeguard the organization. Broader adoption of risk management practices, business continuity planning, and enterprise architecture will follow as a result.

5. Mounting pressure for adequate data protection and security defines public debate

Increasingly, existing standards of the cyber security world will need to adapt to the current threat situation. At the same time, governments are being called to account for their need to have ever more intrusive access to citizen data as a component of cyber strategy designed to defend their country. The EU will continue to evolve its data protection act with scope and enforcement tightening, particularly in relation to data leaving the EU territory. This is likely to lead to a replacement for the recently repealed safe harbor regulation.

Any organization neglecting the security of data transfer from the EU to the United States can expect to attract purposeful attention and attacks by cyber-activists. In addition, the upcoming reform of the EU data protection act will keep it a topic of interest, sometimes interspersed with varying geopolitical and economics positions in light of the recent safe harbor ruling. All of which is still further complicated by discussion surrounding the planned United Kingdom referendum and their membership of the EU.

In Germany, the requirements for data protection and data security for operators of critical infrastructure will become more concrete. It is expected that in spring 2016 detailed legal regulations in the areas of nutrition, water, energy and ICT will be announced. At the end of 2016 industry observers expect further regulations for the sectors of health, transport and traffic, media and culture, finance and insurance as well as state and administration. The

specific conditions relating to reporting obligation and the proof of implementation of appropriate standards of information security will lead to an increased demand for advice from small and medium-sized businesses.

6. Incident response becomes business as usual, so be ready

Traditional 'defense in depth' approaches to information security are no longer effective where attackers are using Zero-Day exploits and Advanced Persistent Threat (APT) techniques. Existing signature-based anti-virus products still have their place, but at best as a hygiene factor.
As we look to the future, new approaches will be necessary to combat the rapidly changing threat environment and develop the capability to recognize continually mutating forms of attack, be it a command server IP address or a malware hash. Organizations hoping to detect an APT at an early stage will need to build (or acquire) the capability to access and analyze vast amounts of data sourced from logs and network packet capture. This will require expert know-how and new tools, with the continued technology trends in mobile, cloud and the internet of things reinforcing this need by driving data flow to increase exponentially. More than ever organizations need efficient incident response structures.

7. Organizations increasingly need to use Managed Security Services

The complexity and sophistication of today's cyber threats means that the majority of IT security teams are woefully under-resourced; lacking the talent and technology to manage the kind of threat-intelligence based controls required to protect their organizations. It is increasingly difficult to find the talent. At the same time, many companies shy away from long-term investment in cost-intensive monitoring and analysis technologies to protect against complex attacks.

An economically attractive alternative is to procure the services of organizations that have already made that investment and provide Managed Security Services (MSS). They provide on-demand, scalable access to state-of-the-art cyber security tools and expertise; while control over internal IT security remains with the consuming organization.

8. Industrial Control System (ICS) Security becomes more important than ever.

On the eve of Industrie 4.0, industrial control system (ICS) security takes on a completely new relevance. Generally speaking, in industrial networks there are often too few security mechanisms implemented - and so they can sometimes provide a comparatively easy point of entry for attackers. The protocols used in industrial networks are robust, but in many cases not assured. In addition, non-routable protocols and networks are increasingly being replaced by routable ones. This particular trend allows remote attackers a seamlessly move around in the network and is further facilitated by the fact that there are often few boundaries between the zones and control mechanisms at the perimeter.

In the context of machine to machine (M2M) communication and the continued dispersion of an organization's network perimeter, it is more important than ever for companies to learn to understand how their office-productivity and production IT systems—a s well as the IT

supporting Industrie 4.0 and the traditional industrial control systems—need to collaborate in the defense of potential attacks. It will require a much deeper understanding of the necessary people, processes, and technologies required to prevent, detect and defend against such attacks, as well as how to effectively execute cyber incident response.

9. Cyber Threat Intelligence becomes essential for information security

The relevance of Cyber Threat Intelligence (CTI), as a part of a proactive information security program, will continue to rise. In response to the increasingly dynamic threat situation, it is critical for organizations to be able to identify the evolving methods and emerging technology trends used by the cybercriminal, and then to continually assess their capability in this regard. Because many organizations don´t have access to internal specialists they will need to turn to external experts from the CTI sector; as they're the only ones with sufficient skills in Open Source intelligence, Social Media Intelligence, and Human Intelligence, to understand the means, motives, and opportunity of modern-day cybercrime, cyber-activism, and cyber-espionage.

Summary

This outlook is the result of a review of current market trends from the perspective of leading security analysts and consultants at TÜV Rheinland, OpenSky, and OpenSky UK. For additional information or to discuss your specific cyber security situation, please contact OpenSky Corporation at www.openskycorp.com.