5 SECURITY CHALLENGES THAT SHOULD BE ON YOUR RADAR

Several, if not all, of these challenges will likely affect you and your organization this year. You should both understand them individually, and look at them as a whole to detect commonalities and opportunities.

#1 – TARGETED ATTACKS

There has been an upsurge in highly targeted, stealthy attacks - one of the most dangerous and potentially damaging forms of cyber-attacks. Security professionals are inundated with security incidents that have revealed apparent risks that extend beyond data exposure to a device, data, and application availability. While some companies are getting better at identifying these attacks, many still find out after the damage has already been done.

DID YOU KNOW?

Targeted attacks are often discovered years after the fact, after thousands—and even millions of customer records or units of information already stolen.

28% of Security Incidents are Targeted Attacks

$400 billion Estimated annual cost to the global economy from cyber crime

"Security professionals are inundated with security incidents, averaging 78 investigations per organization in 2015, with 28% of those involving targeted attacks—the most damaging cyber attacks."

— Tackling Attack Detection and Incident Response, Enterprise Strategy Group, April 2015

#2 – DATA CENTER TRANSFORMATION

Today, most organizations have employees and customers accessing web services, databases, and applications from a myriad of mobile devices and locations. With so many devices connecting to the data center from so many different places, companies have started transitioning their networks from on-premises servers and storage virtualization to the cloud. Rather than adopting a new security solution, many of these companies still apply and leverage traditional security models. To secure their environment, organizations need special protection for software-defined services based on virtual and cloud-based environments, so they don't put themselves at risk.

DID YOU KNOW?

75% of employees chose to use their own device, and almost half are doing so without their employers' knowledge.

40% U.S. employees of large enterprises use personally owned devices for work

51% Employees would go around any policy that restricted use of their own devices or cloud storage

"The lines between work and play are becoming more and more blurred as employees choose to 'use their own device' for work purposes whether sanctioned by an employer or not. Devices that were once bought purely for personal use are increasingly being used for work and technology vendors and service providers need to respond to this."

— Amanda Sabia, Principal Research Analyst, Gartner 2015

#3 – CLOUD SECURITY

The volume of applications and services hosted in the cloud is exploding, and when evaluating new applications for their business, many companies are embracing a "cloud first" delivery approach. Many of these companies are not implementing a strategy to keep data secure and compliant in, to, and from the cloud as a part of increasing "Everything-as-a-Service," shadow IT, and digital business trends.

DID YOU KNOW?

57% of companies say (employee- or company-owned) devices, containing sensitive information, have been lost.

84% of companies have employed cloud-based applications in their offices

40% of firms say they can't effectively manage identities and access management via the cloud

"The key drivers for cloud adoption are organizational agility, cost benefits, and increased innovation. These drivers are offset by persistent concerns about security and privacy, which continue to inhibit adoption, particularly of public cloud services."

— Cloud Adoption Trends Highlight Buyer Preferences and Provider Opportunities
Ed Anderson, Analyst, Gartner

#4 – DATA PROTECTION

Data breaches have become commonplace, and many companies haven't kept pace with growing security challenges. The days of locking down data in the data center are long gone. Today's reality is one of mobile, hyper-connected users on multiple devices. Unfortunately, there have been too many instances where critical business data was lost, stolen or accidentally deleted from an unsecured laptop or USB device. Now, companies must extend their efforts to intellectual property protection, risk management, and proof of due care.

DID YOU KNOW?

Only about 1/5 of corporate data is managed in traditional databases; the remaining 80% lives in mobile devices such as laptops, tablets, and smart phones.

$5.4 million the average organizational cost of a data breach

66% of data breaches took months or even years to discover

"$400 million is the estimated financial loss from 700 million compromised records. This shows the real importance of managing data breach risks."

— Verizon 2015 Data Breach Investigations Report

#5– INTERNET OF THINGS

The Internet of Things (IoT) - a network of physical objects that contain embedded technology that communicates and senses or interacts with their internal states or the external environment - has caused a shift in security. IT security professionals who once only had to protect organizational data and their applications now need to protect their connected devices, along with the data these devices generate. Including billions of connected devices, IoT produces new vulnerable entry points that cyber criminals can access and hack into corporate networks and data, this causing a rise in potential security breaches.

DID YOU KNOW?

The majority of people (87%) have not heard of the term 'Internet of Things'

80% of IoT devices along with their cloud application components don't require sufficient passwords

70% of IoT devices contain at least one security flaw and that the average number of flaws per device is 25

"The growth in IoT will far exceed that of other connected devices. By 2020, the number of smart phones, tablets and PCs in use will reach about 7.3 billion units. In contrast, the IoT will have expanded at a much faster rate, resulting in a population of about 26 billion units at that time."

— Peter Middleton, Research Director, Gartner

THE FIX

intel Security

Each of these trends has inspired Intel Security's adaptive security architecture, a concept brought to life in an integrated security system.

This architecture reduces complexity and improves operational efficiency. It also provides critical integrated, adaptive, and orchestrated intelligence and response capabilities. This means pervasive security from client to cloud and positions you to defeat adversaries quickly.

As a Platinum Intel Security partner, DG Technology is uniquely qualified to formulate a plan, leveraging our expertise, partners, and a unified and open framework for hundreds of products and services from Intel Security and across all security technologies.

LET'S START A CONVERSATION...

About your current infrastructure and your desired outcomes.

813.258.0488

DG TECHNOLOGY

RESOURCES

- http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
- http://www.gartner.com/newsroom/id/2684616
- http://community.hpe.com/t5/Protect-Your-Assets/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.VuMi1XUrJTZ
- https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project#tab=OWASP_Internet_of_Things_Top_10_for_2014
- http://www.gartner.com/newsroom/id/2636073
- http://www.cioinsight.com/it-news-trends/slideshows/byod-is-on-the-rise-but-whos-watching-the-store.html
- http://www.gartner.com/newsroom/id/2881217
- http://www.usatoday.com/story/tech/2014/08/26/byod-bring-your-own-device/14393635/
- http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/enterprise-security-data-protection-paper.pdf