
STRATEGIC
SECURITY
A DG TECHNOLOGY PUBLICATION
THE TOP CLOUD SECURITY CHALLENGES FACED BY IT PROFESSIONALS
RETHINKING DATA SECURITY: WHAT TO CONSIDER BEFORE YOU'RE HIT
HOW TO BE PREPARED WHEN RANSOMWARE HITS HOME
5 SECURITY CHALLENGES THAT DEMAND YOUR ATTENTION
DG
TECHNOLOGY

CONTENTS

5 SECURITY CHALLENGES
THAT DEMAND YOUR ATTENTION

Identifying top concerns and security issues that should be on your radar.

The advent of cloud-based services, increased use of smartphones, appliances with Internet connections, and increased cyber theft and espionage from foreign agents have combined to create a tsunami of new security challenges for IT managers. Unfortunately, there's not a single solution to thwart each new attack. Existing technologies in place at most companies are ill-suited to address increasingly sophisticated attacks and new security concerns.

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 dealt with an average of 78 security investigations per firm in 2015, with 28% of those involving targeted attacks, according to a survey by the Enterprise Strategy Group in April 2015. The numbers are only expected to increase in 2017.

These attacks aren't coming through network perimeters protected by firewalls, but often arrive through email, web posts, network files, instant messaging, file share cloud programs, databases, desktops or laptops, removable media, printers, smart phones and cloud email, storage, and even partner agencies. Firewalls don't protect all these different access points, and most virus software doesn't either — leaving many companies vulnerable.

Many companies don't detect targeted attack breaches until weeks, months and even years later. Part of the problem stems from the very complicated and timely process it takes to detect these violations. Companies have put in place an array of security devices from different vendors that don't talk to each other, making it hard for IT to gain visibility into the entire ecosystem and making it hard to manage and find intruders.

2) DATA CENTER TRANSFORMATION

The data center is the heart of most businesses, but many aren't set up to handle remote access, cloud computing and other functionality that's been created in the past few years. Most data centers have been virtualized, consolidated and centralized, and now must become more open, service-oriented and modern to meet the needs of a growing mobile workforce.

THE CHALLENGES

A modern data center must host critical applications and data, help employees consume IT as a service, and augment capacity by using an external cloud. Companies need special protection for software-defined services based on virtual and cloud-based environments to secure this new way of doing business and avoid putting themselves at risk.

3) CLOUD SECURITY

According to security firm SailPoint, 84 percent of companies have cloud-based applications in their offices. These applications allow them to be more agile, spend less on IT and boost innovation, says Ed Anderson, an analyst at Gartner.

But he states, "These drivers are offset by persistent concerns about security and privacy, which continue to inhibit adoption, particularly of public cloud services." About 40 percent admit they can't effectively manage identities and access management via the cloud, leaving them vulnerable to security breaches.

Complicating this issue further is the fact that employees often use cloud services of their choice without the knowledge of IT or even their bosses. They upload and share data with partners or even co-workers and are often unaware of the security protocols they should be following.

4) DATA PROTECTION

Only about one-fifth of corporate data is managed in traditional databases, the remaining 80 percent lives in mobile devices such as laptops tablets and smartphones. Most companies don't have a good inventory of where their data resides, and they also don't know if it's protected.

Some have installed data loss prevention technology, also known as DLP, thinking DLP will find issues for them, forgetting that they need to put policies in place to make the technology useful. Putting those policies in place means they have to identify critical company data, figure out where it resides, determine who has — and who should — have access to it, among other things, which some try to avoid since it is a time-consuming process.

According to Verizon's 2015 Data Breach Investigations Report, the estimated financial loss from 700 million compromised records was $400 million. That staggering figure illustrates the real importance of managing data breach risks.

5) INTERNET OF THINGS

Remember the Target breach? Cyber thieves didn't directly attack the retailer's corporate network. They slipped in through an Internet connection with stolen VPN credentials a small heating and cooling vendor used to check Target's refrigeration units. Certainly, you've heard about the people hacking into computer systems in cars, right? Just when you thought you had your arms around the devices connecting to your corporate network, the Internet of Things or IoT is opening Pandora's Box to an endless number of new entry points

By 2020, the number of smartphones, tablets, and PCs in use will reach about 7.3 billion units, says Peter Middleton, Research Director at Gartner. In contrast, the IoT will have expanded at a much faster rate, resulting in a population of about 26 billion units at that time, he says.

Even scarier: 80 percent of IoT devices and their cloud application components don't require sufficient passwords. Making matters even worse: 70 percent contain at least one security flaw, and the average number of flaws per device is 25 percent. Securing your network and company is going to get even more complicated.

McAfee™
SECURITY

RETHINKING SECURITY: A NEW, CONNECTED ERA

These new security threats have caused McAfee to rethink the way it provides security solutions. The company is creating an integrated and adaptive security system that reduces complexity, offers increased visibility and improved operational efficiencies. McAfee is working with other security vendors and has proposed a standard set of protocols that connect vendors and products on-site and in the cloud, making it easier to manage security.

How to be Prepared WHEN RANSOMWARE HITS HOME

RANSOMWARE INFECTIONS ARE HAPPENING MORE & MORE.

It's not a matter of if you will get hit, but when.

WHAT'S HAPPENING TO COMPANIES GETTING HIT BY RANSOMWARE?

Hospitals in Los Angeles, Kentucky and West Virginia are just the latest firms to get hit by Ransomware, a type of malware that prevents or limits users from accessing their systems until a ransom is paid. Unfortunately, this type of cyber-attack is increasing rapidly. While many businesses don't think their small or relatively unknown companies could be targeted, the opposite is actually true. It's not a matter of if you will get hit, but when.

Recently, a local organization was struck. They were unable to restore the data from backup and was forced to pay the ransom. Luckily for them, the ransom wasn't that much and they received the data back. Thieves like to keep the ransom amount relatively low in many cases because they believe in doing so, they are more likely to get paid.

This organization engaged us to help them work through the problem and we discovered they had many gaps in their security controls, and unbeknownst to them, other malware on their system waiting to strike again. We rebuilt their entire security infrastructure and strengthened their endpoints because they were so vulnerable.

Ransomware infections are happening more and more in part because traditional antivirus software is unable to detect this malware. It operates in stealth mode and often bypasses basic security controls. It often arrives through people who browse the Web with outdated Web browsers and/or browser plugins like Java and Adobe Flash and Reader. Ransomware originators often gather personal information and use it against unsuspecting people by making an email appear from a friend or coworker, and ask for information or to click on a link, which opens the door for an attack. With an ever-evolving threat landscape,

4 THINGS YOU DO TO PROTECT YOUR COMPANY

01 Don't just back up your critical data, make sure that the backup is working properly and that you test your data restore processes. It's the restoring part that usually gets overlooked by many companies. So, test your entire system, make sure that your system can restore your data and then test that the data can be accessed after its restored.

02 Continually train your employees on safety best practices, including hovering over links to make sure they are properly identified and to make sure they don't download any file from someone they don't know. This doesn't just pertain to desktop machines, but smartphones, tablets and any internet connected device. If your employee did win Powerball, they probably wouldn't be notified via email; nor would their inheritance be routed through a different country. This type of training should be done on a regular basis, not just annually. To determine who might be vulnerable to this type of attack, perform a phishing test as a foundation for further education.

03 Audit your computer system and network to make sure you know and understand where your greatest vulnerabilities lie. One antivirus software product will not protect your entire infrastructure. Security today demands a layered approach with various controls.

04 Because most malware comes through email that asks users to click on a link or download a file, make sure your security blanket includes products that monitor email, web sites and web traffic.

it's more important than ever that companies reassess their security strategies, make sure they have an up-to-date audit of their security defenses, and have a continual plan in place to update and train employees on security best practices. No one in your company should still be using "password123" as their password, for example. Even just one instance of this password can be a conduit for widespread risk.

ALWAYS USE A COMPLEX PASSWORD TO PROTECT YOUR DATA.

CLOUD SECURITY

THE TOP CHALLENGES FACED BY IT PROFESSIONALS

Security-as-a-Service provides IT security professionals with multiple options to safeguard critical data, detect breaches, and deploy corrective solutions. With SaaS and IaaS (Infrastructure-as-a-Service) solutions being deployed across organizations of all sizes, the adoption of Security-as-a-Service still faces challenges. These are some common questions and challenges faced by IT security professionals that still may be hesitant about adopting a cloud-based security platform.

The Cloud is Still Unknown

IT security professionals want a transparent cloud security provider. The biggest adoption challenge relates to IT security professionals not understanding how cloud providers actually keep data centers secure. IT senior management wants more transparency from cloud service providers so they can make better informed choices about how to procure the best security resources with budget constraints.

Management is Unsure and Worried About the Public Cloud

IT security professionals find that less than half of senior IT management understand public cloud risks. C-Suite executives, who are responsible for developing cloud budgets, have even less of an understanding of public cloud security.

The Cloud is Not Being Secured

The cloud isn't being secured. 43% of IT security professionals do not use encryption or anti-malware in their private cloud servers. 38% utilize IaaS (Infrastructure-as-a-Service) without encryption or anti-malware. 40% do not institute a DLP (data loss prevention) program with files located on SaaS architecture.

Security-as-a-Service is a Top Investment Priority

Despite challenges in full or hybrid cloud security adoption, 78% of IT managers plan on investing in Security-as-a-Service. Only 35% of IT departments are employing an integrated security solution. This number will increase as budget allocation changes.

> ***Less than half of senior IT management understand public cloud risks.***

Other Difficulties

The SANS survey reports that IT security professionals are having difficulties in other areas of cloud adoption. The top categories are:

- Difficulty migrating services or data (27%)
- High costs and fees / poor value (25%)
- Lack of visibility into cloud provider operations (25%)
- Visibility into security incidents (23%)

The Private Cloud is the Favorite

While only 13% of IT senior management trust the public cloud, 37% completely trust private cloud. For enterprise and large-sized organizations, a private cloud solution will be favored by IT professionals who need to also worry about being compliant with various legislation. Public cloud solutions, which may be more flexible for small to mid-size organizations, will likely need a stronger business case.

Adopting a Security-as-a-Service Cloud Solution

Securing data and operations in the cloud is the number one priority for IT professionals, management, and C-Suite executives. Whether you need a private, hybrid, or public cloud solution, DG Technology can assist you in making the best choice for your business. Through our robust solutions options, we can create a functional cloud security operation that can quickly scale in response to mounting cyber security threats.

RETHINKING DATA SECURITY

What to Consider Before You're Hit

WHEN WILL YOU GET HIT?

Seagate, Ashley Madison, eBay, AOL, Target, Home Depot, Sony, the U.S. Government, and JPMorgan Chase. Now, insert your company name at the end of the list. It's not a matter of if your corporate data will be targeted by cyber-criminals, but when.

The question is, are you going to wait until you're hit or are you going to take a proactive approach to bolstering your data security before your company ends upon the hit and headline list?

Most companies wait until a data breach happens before they take steps to better protect their data.

WHAT YOU MAY NOT UNDERSTAND

Unfortunately, most companies wait until a data breach happens before they take steps to better protect their data. Why? Because many don't realize relying on old practices and technologies is not enough to thwart modern day thieves who are getting more sophisticated by the minute.

They don't understand that data is different and needs special attention. Many rely on technologies like a firewall to thwart cyber thieves, forgetting that a firewall won't stop thieves from tapping into the CEO's smartphone or marketing's use of cloud-based storage solutions like Dropbox.

If you are among the savvy companies that want to proactively protect your data, you need to know what you should be doing differently today to improve data security and prevent data loss.

UNDERSTAND DATA IS SPECIAL

First, you need to recognize that data is different, and special. Many security products, like a firewall, for example, are just one piece of a greater puzzle – one product doesn't stop all breaches. Most likely you don't have, but need a data loss prevention product, known in the industry as DLP, to fortify your defenses. It operates much like your home's smoke detector, increasing your protection from a fire.

CONSIDER ADDING A DLP

Solutions like McAfee's DLP identify, monitor and protect data in use, as it moves on your network, and as it sits on desktops, laptops, mobile phones or tablets. DLP systems are like the police; they enforce data security policies through contextual

DATA LOSS PREVENTION SYSTEMS

DLP systems enforce data security policies through contextual analysis and content inspection.

analysis and content inspection. DLP provides a framework – guided by your policies – that detects and prevents the unauthorized use and transmission of your critical data – much like police enforce laws. DLP also protects against internal mistakes and intentional misuse by insiders and external attacks.

POLICIES ARE CRITICAL TO DLP SUCCESS

DLP isn't a technology you simply deploy and forget about. You need to create corporate policies so the system understands policies such as who is allowed to download and distribute certain critical information, who is allowed to access certain data and so on. Without the policies, the technology isn't going to protect you.

What policies do you need to implement? Some will be obvious – your cleaning crew, for example, doesn't need access to the daily sales report. Other policies won't be as obvious, so bringing in a trusted consultant with experience will no doubt save you time and the headaches that come with trying to figure out what's needed on your own.

KNOW WHERE YOUR DATA RESIDES

Before you can protect your data, you actually need to figure out what data you want and need to protect, and where that data lives. While that sounds simple, it's actually a complex problem. For example, have you asked every one of your employees to reveal:

- Which email systems they've used for corporate email
- How many USB drives they own with corporate data on them
- Which cloud storage systems they use
- How many web posts they've created and where they are
- What the folder system looks like on their desktop and laptop
- Whether they've used their smartphone for work
- Which partner agencies and independent consultants that they have shared corporate information with

Probably not. But take a look at that list and you'll realize how hard it is these days to know where your corporate data resides, and how much of an overwhelming task finding it and classifying it might become when you have hundreds and thousands of employees and partners.

START WITH A SINGLE DEPARTMENT

Some vendors will tell you to classify your data before you can adequately protect it. What they don't tell you is that it can take years to classify data. Some companies are stuck trying to find and categorize their entire data repository leaving them exposed to hackers. Instead, we advise you to start small, with a department like human resources and build from there, identifying where critical data resides and then building policies around it. That's what we did with a midsized, rapidly-expanding-through-acquisitions logistics company with some 10,000 users. Because the company worked with several federal agencies, executives needed to prove the company had a program in place to protect customer data as part of its compliance certification. Executive buy-in was already in place.

Rather than launching an ambitious data classification project, we divided the company and started with a rather simple part, human relations. We helped them identify what their critical data was, where it resided, and crafted policies to protect it. This helped us establish a baseline and helped other departments understand how data impacts operations and how the process would work for them, which eliminates some of the fear involved in the project. Users need to see that we aren't taking access to data away from them or locking it up but better protecting it.

HOW TO KEEP UP WITH CHANGING SECURITY LANDSCAPES

With the average cost of a data breach now at nearly $3.8 million, and attacks coming faster and furiously, it is more important than ever to secure your data. Keeping up with the latest security measures is difficult. Good security experts are hard to find and expensive to hire, so many companies are turning to trusted partners to help them navigate the rapidly changing security minefield. With an overall understanding of where your data lives, DLP technology, and trusted partners that can help you implement the correct policies, you can avoid becoming the latest security breach headline.

Five Reasons to
ASSESS YOUR SECURITY RIGHT NOW

FACTS ABOUT SECURITY BREACHES

Security threats seem to scale in proportion with security solutions. These facts about security breaches are a reason to assess the current state of your IT security and consider how cloud-based solutions can provide added defense against data breaches.

It Takes a Long Time to Find Out Data is Missing

Data breaches target critical information such as healthcare records, customer credit cards, accounting data, and employee information. On average, it takes 150 to 180 days to spot a data breach. In this scenario, data is being accessed and sometimes sold for six months before internal IT staff recognize the intrusion.

The Bigger the Organization, The More Daily Incidents Reported

Organizations experience up to 20 incidents per day, sometimes more. A single undetected incident can give attackers access to a treasure trove of critical data.

> ***Roughly half of employee related breaches are accidental and the other half intentional.***

Breaches Are Expensive

The average cost of a data breach is largely unknown, with most organizations reporting a cost-per-record of $80 to $400. However, the cost of a breach extends far beyond the compromised records. A report by Deloitte on the hidden cost of breaches shows that:

- Organizations face increased insurance premiums after a breach.
- There is a strong association between data breaches and brand devaluation.
- Many organizations face a loss of intellectual property, limiting future income streams.
- Business-to-business relationships suffer, especially when it comes to partnerships and contracts.
- Consumers impacted by the data breach lose confidence and ultimately may look to competitors for similar products and services.

> ***Roughly half of employee related breaches are accidental and the other half intentional.***

Employees Are the Biggest Point of Breach

A majority of data breaches originate within the organization. In 2015, an estimated 59% of reported security breaches involved employee fault (this includes employees, contractors, and third-party suppliers). Employees who have unnecessarily high level access, accidental malware downloads, and compromised credentials make employee access points the most common point of origin for data breaches.

THE PROMISE OF CLOUD-BASED SECURITY

A 2016 SANS survey showed that cloud data breaches were down to 9% when compared to traditional, on premise IT security systems. Data breaches remain the top priority for organizations, making cloud-based security the best solutions architecture for organizations that need flexible, responsive data protection options.

No Data is Left Untouched

Once a malicious actor has access to critical data, the most valuable data is exfiltrated first. Since it can take months to realize a breach has occurred, many actors can obtain access to multiple levels of critical information.

The McAfee sponsored cyber threat report, Grand Theft Data, finds:

- Intentional internal breaches take employee records (33%) followed by customer information (27%).
- External actors take customer information (32%) and employee information (28%).

This suggests that credit card data, social security numbers, telephone numbers, and addresses are the most valuable targets for internal and external breachers.

There is incredible value in taking a 'back to basics' approach to endpoint security.

INCREASE SECURITY: LOCK DOWN USER PRIVILEGES

Focusing efforts on the fundamental aspects of security helps create a rock-solid, network foundation without the costs associated with procuring new hardware or software.

TRAVIS ABRAMS

Today, users are often on the front lines of the cybersecurity battle because they're some of the easiest targets. Instead of attacking a complex software vulnerability, hackers use social engineering techniques to create extremely convincing email messages to users that contain files designed to infect machines with malware, or they include links to compromised websites, which extract information.

IT can help protect vulnerable users and secure data from social engineering and malware by placing a big emphasis on assigning proper roles to each user — and removing administrator privileges — so malware cannot be executed.

How Account Management Helps

Typically, when a device becomes infected with malware, it's because the malicious code exploited vulnerability, or it was executed on a machine with administrator privileges. It's much easier to target user machines and hope they have the right level of privileges, rather than try to exploit an advanced (and unpatched) vulnerability. In fact, when leveraged by cybercriminals, user rights can act as a key vulnerability, granting intruders access to execute malicious software, while gaining a foothold for a larger attack. Limiting user privileges on company hardware helps keep networks safer because it can contribute to restricting the scale of potential breaches, isolating them to a single device, or hopefully preventing them before they even start.

It goes without saying that in highly regulated environments such as the public sector, controlling user privileges should be a top priority. However, this essential IT function should not be overlooked by other organizations.

> ***67 percent of organizations indicated they had seen an increase in attacks.***

> ***93 percent of organizations reported they were unable to triage all relevant threats.***

Make the Most of Your IT Team's Time

In the latest McAfee Labs Threat Report[1], 67 percent of organizations indicated they had seen an increase in attacks and 93 percent reported they were unable to triage all relevant threats, a clear sign they are overwhelmed by the sheer number of security incidents. A recent McAfee Cloud Report[2] also suggests there is a shortage of security professionals, with 49 percent of organizations saying they had slow adoption of cloud services because of a lack of security skills.

A back to basics approach to security can help ease the burden of a rise in security incidents on IT teams by preventing many issues from happening. From network visibility to data protection and user management, the three tenets — network visibility, data protection and user management — of this approach focus on the fundamentals of a secure enterprise network.

The Role of Education

In many ways, education is just as important as network visibility, data protection, and user management, but it is often a longer-term project. Teaching users about security best practices is an excellent preventative measure and worth the investment because users can help identify sensitive data and help prevent breaches.

Educating users in security best-practices is also an ongoing, long-term strategy and requires executive-level support to be truly effective, but is a worthwhile pursuit.

[1] https://www.mcafee.com/ca/resources/reports/rp-quarterly-threats-dec-2016.pdf
[2] https://www.mcafee.com/us/solutions/lp/cloud-security-report.html

DG TECHNOLOGY

Securing critical data, applications & infrastructure from device to cloud.

(813) 258-0488 | www.dgtechllc.com