SECURITY CONCEPTS FOR A DIGITAL WORKPLACE

A deeper look into cyber security, the threats you'll face, and how to fight them head on

888-435-7986 | www.getgds.com

GLOBAL® DATA SYSTEMS

INTRODUCTION

> **I often have conversations about cyber security, even with those who are not focused on the protection of systems and data.**

So little is known or understood that people are often unaware of the threats around them. Most people just don't see them. In a discussion regarding the compromise of a student records platform at a school, the general attitude was "So what if some student records are changed?" - "How bad can that be?"

If we consider that these individuals will become adults with a credit history, then we can see that this could be the origin of an identity theft exploit.

The focus of this white paper is to shed some light onto a very dark topic – cyber security.

THE EVER-CHANGING ATTACK SURFACE

A few decades prior to the creation of the public Internet, institutions such as education, military, and some R&D sectors created a foundation for a new way to communicate – Internet Protocol.

It certainly expedited our pace of communication but, like many communication methods available at the time, it lacked a security element.

- Is the person sending the message **known to be trustworthy?**
- **Has the message been altered** along the way?
- Did prying eyes get a **glimpse of confidential or propriety information?**

Through the decades, security has been evolving to address these shortcomings. Early improvements encrypted data in transit, preventing modification or theft of data. More layers, such as guaranteeing the authenticity of the sender have been added over time.

Billions of Connected Devices

As corporations adopted electronic, online business practices, the number of devices have grown exponentially. By 2020, there is expected to be 50 billion devices connected to the Internet – more than 7 times the world population of humans. Every device can be a source, target, or unwilling accomplice in a security attack or breach. The Internet of Things (IoT) is in large part the reason for this explosive growth. We have transitioned away from human-to-human communication and now include variations such as human-to-machine, machine-to-human, and machine-to-machine. A typical consumer will have a laptop, smartphone, smarttablet, plus wearable devices such as health monitors, activity monitors, watches, etc. All these devices are designed to create, store, transmit and display information.

As we put our personal or corporate information on this global network, we open ourselves up to become victims of activities ranging from identity theft to corporate espionage.

Growing Attack Surface

A recent, well known credit card theft activity didn't actually originate with any banking, credit card bureau, point of sale (POS), or related system. The attack vector (entry way) originated with the controls of a heating, ventilation, and air conditioning system (HVAC). The attackers focused on a system that had very little security built into it because of its seemingly benign nature. It did not process any personal data, financial transaction data or anything of value to anyone but the facility managers. Once the HVAC system was penetrated, however, a sophisticated and focused attack on a POS system on the same network allowed the intruders to harvest credit card information for millions of shoppers. If we look around us and notice the devices we use today - vending machines, parking lot payment systems, biometric monitoring systems, etc. – we can see that the attack surface is growing rapidly. These are just examples of human-machine systems. Manufacturing, retail space, education, healthcare, transportation – almost any industry that can be conceived of – depends on a wide range of machine-to-machine systems.

As the attack surface continues to grow, we need to view security in a new light. It needs to evolve from trying to protect a business to enabling business.

ADVERSARIES

Another area of explosive growth is multi-billion dollar a year hacking industry.

From 2013-2016, business e-mail compromise alone generated more than $5.3 billion in revenue. Ransomware brought in more than $1 billion in 2016. The hacking community has developed into a mature supply chain model where code developers are no longer the attackers.

Anyone can purchase a hack and deploy it with minimal technical skills. A $100K investment can produce millions in return. Long gone are the days of a "lone attacker" working in isolation. Even nation states have joined the attack force. Foreign states actively recruit hackers and invest to reach their end goals – whether they are financially or politically motivated.

Prepare, Detect & Respond

Given the growth in attackers, one may wonder if they can ever be truly secure. After all, the attackers only need to be correct once to execute a security attack. The victim must be correct at all times to successfully prevent an attack. Conclusion: you will be hacked. How you survive an attack will depend on how you prepare, detect and respond.

The stated goals should be to:

1. Limit the number of successful attacks
2. Decrease the time to detection of a breach
3. Gain visibility to files or data sets compromised in the breach
4. Quarantine and remediate

A properly designed architecture helps protect every area of your business, from the data center to the network edge to cloud applications.

There are hundreds of security vendors in the market, each with a number of products to secure a portion of your network. The network architecture should consist of solutions that are deeply integrated, working in tandem, and have the same security intelligence feed from a central research group. Below are key product types and their focus area:

Firewall/Next Generation Firewall (NGFW)

The firewall has been the single greatest threat protection for decades. Its function is simple, only allow permitted traffic through. As attack sophistication has increased, the NGFW has emerged. Not only does it permit specific traffic through, it further analyzes the traffic to ensure that it is safe. For example, web traffic may be permitted but malware from an infected website would be denied.

Advanced Malware Protection

Building on the NGFW inspection capabilities, AMP continuously analyzes file activity across your extended network, so you can quickly detect, contain, and remove advanced malware. The firewall is not the only attack vector for malware so it cannot be the only enforcement point. Portable drives and laptops, tablets, and smart phones in use outside of the protected corporate network are common entry points for malware.

Email Security

Email is the most common attack vector for malware. It accounts for more than 85 percent of malware entering an organization. Two common threats are:

1. **Business email compromise attacks that masquerade** as a corporate executive to authorize payment of a fake invoice
2. **Ransomware** – that encrypts corporate data and demands payment prior to decryption.

An Email Security system is a key resource to prevent these attacks.

Network analytics

Not all networking devices have a specific security function. They do, however, see all the traffic passing through the network. Think of these devices as "sentries" detecting a change in behavior that is congruent with an attack. They can report this change in behavior to security management systems to take further action. After all, you cannot manage what you cannot see.

Policy and Access

The focus here is to determine who, what, when, and from where your network can be accessed. It is not enough to determine who a person is prior to accessing resources. You should also determine what device they are using and if it meets corporate standards for operating system versions, security patch levels, anti-virus signature, etc. You should have complete awareness, context and control of everything that is hitting your network.

Web

Keeping track of threats and vulnerabilities is a daunting task. **Advanced web filtering allows an organization to stop vulnerabilities in real time.** It also allows for "back tracking" of vulnerabilities that were not yet classified when downloaded. Tracking the destination of these files is key to handling zero day threats. As they are identified as threats, you need to know where they went in order to quarantine and remediate them.

DNS

The Domain Name System has been around for decades. Its function is simple it helps people navigate the internet. You enter a URL in your browser and DNS gives you directions to reach that resource. **Filtering out responses that are known to direct people to malware-infected sites** or unauthorized content such as like gambling, social media and pornography, is a key first step in securing your network.

CONCLUSION

You are probably realizing that security is not a "set it and forget it" activity. It takes planning, preparing, responding, and a constant re-evaluation of threats.

Most organizations do not have the resources for this level of activity so it is imperative that you select the proper products to be protected.

GDS has developed a suite of managed security services that effectively address the primary threat vectors.

Our cloud-based tools are **designed to prevent network intrusions, protect email and end-user devices, block malicious websites and files, and analyze user behavior** to detect compromise.

GDS can help you protect your business
Contact Global Data Systems: 888-435-7986