QUARTERLY SECURITY REPORT

2020

CISCO Partner

ROBINETT CONSULTING

robinett-consulting.com

Introduction

Robinett Consulting knows having a proper defense against cyber security threats is critical to preventing potential loss to your business. To keep your company safe, we take a layered approach by first assessing your risks and then providing the proper protections best suited for your situation. Whether you are a small business or an enterprise company, we customize the solution to your specific security needs. This report outlines just three security layers and some of the solutions we offer that you should know about for properly protecting your business: Edge Protection, Multi-Factor Authentication, and Dark Web monitoring.

Edge Protection

Proactive Protection

The perimeter of an organization is a common vector for attacks. Attackers must get through the edge to get to valuable assets: proactive security here mitigates risks and reduces your exposure.

Small businesses are hit by **62%** of all cyberattacks

Perimeter Security

Edge Protection acts like a guard post and patrols along the perimeter of a secured area. This security deters attackers and is a major proactive defense for protecting your environment.

WHAT DOES IT DO?

Edge Protection can mitigate risks from:

- Malware such as Ransomware, Trojans, and Viruses.
- Websites that contain threats to your devices.
- Remote hacking attempts on local devices.

Solutions:

The following Edge Protection solutions are Cisco firewalls backed by Talos. Talos backs all Cisco products and is comprised of world-class researchers, analysts, and engineers; they are one of the largest threat intelligence teams and an industry-leader in threat intelligence.

Meraki Firewall

KEY METRICS:

- Simplified management within a seamless single pane on a web browser.
- Tailored for SoHo and Branch sites.
- Next Generation Firewall and IPS.
- Can be managed by web browser in the cloud.

Adaptive Security Appliance

KEY METRICS:

- Traditional/Stateful Firewall.
- Multi-context Firewall
- Remote Access VPN Headend.
- Upgradable to Next Generation capabilities. Can be managed by CDO or ASDM.

Firepower Threat Defense

KEY METRICS:

- Next Generation IPS.
- Next Generation Firewall.
- Advanced Network Visibility and Threat Analytics.
- Incident response and threat investigation.
- Can be managed by CDO, FMC, or FDM.

What Edge Protection Keeps Out

Malware, short for malicious software, is a catch all term for software that is specifically designed to disrupt, damage, or gain unauthorized access to a device or network. Malware programs can cause a variety of problems for your devices such as providing an access point for malicious actors or more specific forms of Malware such as Ransomware or crypto miners. In short, Malware will take control of your devices to do anything from taking control of your environment to stealing information.

Ransomware, for example, has been a devastating malware attack on businesses large and small. Malicious actors will gain some form of profit by holding a company's data hostage and causing the business to grind to a halt. The business will begin hemorrhaging money, and the malicious actors will utilize fear tactics and social engineering during the attack to have their demands met. Dire situations such as this are why Ransomware should be taken seriously by all businesses and proper mitigation put into place to help prevent company doors closing.

Regardless of the size or age of a company, they are all targets, and this is seen with The Heritage Company.[1] When The Heritage Company got hit with Ransomware, they ended up paying the ransom which caused the loss of hundreds of thousands of dollars and employee layoffs.
When thinking about protection for your business, it is important to know that Ransomware can only wreak havoc if it takes control of your machine, and one of the first points to mitigate ransomware from entering the environment is the edge. Proper Edge Protection can help mitigate ransomware before it enters the environment and before it has a chance to take hold. Listed here are a few more examples of malware that edge protection will keep out of your environment.

TrickBot[2] is a Trojan malware that attempts to install backdoors into machines, and a new technique has improved the malware that allows it to evade newer security controls to accomplish its task. This new evasion technique allows TrickBot to threaten even the most secure networks with a backdoor.

Oski[3] is a data-stealing malware that specifically targets credentials, credit card numbers, crypto wallet accounts, and more. North America and China are currently Oski's main targeted areas.

Emotet[4] has always been highly prevalent and has had a new 'evolution' that allows it to spread to local unsecure WiFi networks. This propagation allows Emotet to spread at a high rate and attempt to brute force devices on those networks. Credentials are the main target of this malware and, with the ability to cover a wider area, its risk to devices increases dramatically.

Anubis[5] does not limit itself to just one action like the previous malware examples— it steals credentials and acts as ransomware. Unlike other malware that attack desktop or laptop devices, Anubis targets mobile devices, specifically attempting to steal credentials to banking apps and then potentially hold the mobile device for ransom. Examples like this are why having mobile device protection is a requirement for today's landscape.

Overall, Edge Protection is an invaluable first layer of security because stopping the threat at the door prevents it from becoming a bigger issue in the future. The key idea to remember is that you want to proactively keep malware out rather than deal with it once it is inside your environment.

[1] https://threatpost.com/ransomware-attack-topples-telemarketing-firm/151530/
[2] https://threatpost.com/trickbot-custom-stealthy-backdoor/151663/
[3] https://threatpost.com/oski-data-stealing-malware-north-america-china/151856/
[4] https://threatpost.com/emotet-now-hacks-nearby-wi-fi-networks-to-spread-like-a-worm/152725/
[5] https://threatpost.com/phishing-campaign-targets-250-android-apps-with-anubis-malware/152666/

Multi Factor Authentication

Strengthened Security

Having a reliable Multi-Factor Authenticator (MFA) is important because even if you have strong passwords, your credentials are still at risk.

Your passwords for third party sites might be encrypted, but they must be stored somewhere, and the security of that storage can be compromised without you being immediately aware.

HOW IT WORKS

To mitigate the danger of compromised credentials, MFA secures your account by requiring a second form of verification, such as a smart phone, to allow access to an account.

This means that even if your password becomes compromised, it will be much more difficult for your account to be stolen by an attacker.

To add a layer of security that allows your company to easily meet compliance for access and user authentication controls, Robinett Consulting offers Duo, Cisco's Multi-Factor Authenticator.

Easy Implementation

KEY METRICS:

Duo protects many programs your business implements and provides secure access to your applications.

Once you have gotten started with Duo, your users will have a variety of authentication options that allow for security without interrupting their individual workflow.

Scalability

KEY METRICS:

Duo's self-enrollment feature for company members makes deploying and implementing Duo easy and worry free. This also means that as your company grows, Duo enrollment will easily scale with your growth.

Control and Monitoring

KEY METRICS:

Duo allows you to differentiate personal and business devices, assess the security of all devices, and identify then monitor potentially risky devices.

In addition to this, you can implement role-based access to control which devices can access applications based on hygiene or ownership.

MFA Real World Examples

Credentials can be stolen numerous ways and it is not always preventable. One of the uses for stealing this data is to use that stolen information to obtain even more information. One set of stolen credentials means that anywhere those credentials are used now becomes a target. This can lead to a cascade of breaches into accounts ranging from shopping accounts, banking accounts, and your company's internal systems.

Proactive protection is what MFA provides, and is an additional layer of security. The MFA layer of protection helps prevent compromises and can protect accounts even if credentials are stolen. Listed here are examples of companies that had their credentials phished with disastrous consequences, but if they had an MFA, they would potentially have prevented a breach.

Sinai Health System

A phishing attack compromised company credentials and went undiscovered for months. Names, addresses, dates of birth, Social Security Numbers, health information, and health insurance information leaked because there was no extra layer of security to prevent access with the compromised credentials.

Synoptek

A phishing attack allowed the access necessary for a Ransomware attack. No personal information was stolen, but the company lost face in the public eye as a result.

Special Olympics NY

Phished credentials allowed malicious actors to access the company's records and send a subsequent phishing attack to previous donors to the organization.

Manor Independent School District

Phished credentials were used to access the district's environment and siphon millions of dollars from the district.

Dark Web Monitoring (DWID)

Credentials for accounts can be found on the Dark Web for less than a small coffee. Once bought, access to these credentials can cause a business to close their doors.

What is the Dark Web?

The area of the internet that you access every day is just the surface of the internet. Underneath is the deep web and the Dark Web; it is in the Dark Web that a wealth of stolen data circulates for sale.

The average cost of a compromise for SMBs in 2019 was ***$1.24M***

How would your credentials end up on the Dark Web?

- Your credentials can be keylogged or phished when entered on a fake website or stolen by malicious software.
- 3rd Party Data Breaches will leak a large amount of information when an outside website or data base that holds information related to your credentials is hacked.
- Accidental and Malicious Exposure are also risks as your data may inadvertently or intentionally be shared on the internet.

58% of SMBs say they do not have visibility into employees' password practices

You can't control a data breach, but you can control if that data is still valid. To monitor and mitigate the threat of stolen credentials, Robinett Consulting offers 24/7 monitoring with Dark Web ID.

What does DWID do?

DWID alerts you when your information is found on the Dark Web. The earlier you know what information is out there, the sooner you can secure your credentials.

You may not be aware that your credentials are on the Dark Web, but, if they are, we will let you know and inform you of any personal information that has been leaked along with those credentials.

Dark Web ID scours the Dark Web to find your information on:

- Dark Web Chatrooms
- Hacking Sites
- Hidden Theft Forums
- Peer-to-Peer file sharing networks
- Other Black Market Sites

Real World Examples

Data breaches are a matter of when and not if they will happen, and data breaches come in many forms, whether it be accidently losing a physical letter or an entire database being copied and stolen. The responsibility for protecting a client's data from being stolen rests with the company, but malicious actors are aggressive, cunning, and always on the lookout for an opportunity to steal data and put it on the Dark Web.

Listed here are a few cases where there was a breach, and data, personally identifiable information (PII), and credentials were put out on the dark web to be sold for less than a small coffee. If these businesses were utilizing DWID, their stolen credentials might have been caught earlier and attacks prevented.

Alomere health

Phishing revealed the following PII: names, addresses, dates of birth, medical record numbers, health insurance information, and sensitive diagnosis and treatment details. In addition, some patients had their Social Security numbers and driver's license numbers exposed.

The Center for Neurological and Neurodevelopment

Successful phishing allowed attackers to gain the credentials necessary to enter the environment, and they had unauthorized access for over a month.

Royal Yachting Association

Attackers infiltrated the company's network and downloaded a database. This database contained PII for the customers and this information can be used in the future for different attacks.

SuperCasino

Attackers breached a database that contained PII and had access to names, usernames, email addresses, telephone numbers, residential addresses, and account activity data. This can be used in the future against these individuals.

Conclusion

Proactively protecting your business can be challenging and complicated, but it is a necessity in today's world of tenacious and creative attackers. Do not be another statistic, do not be low hanging fruit, and do not be a victim to cyber-attacks. Please contact Robinett Consulting for more information.

ROBINETT CONSULTING

robinett-consulting.com

CISCO Partner