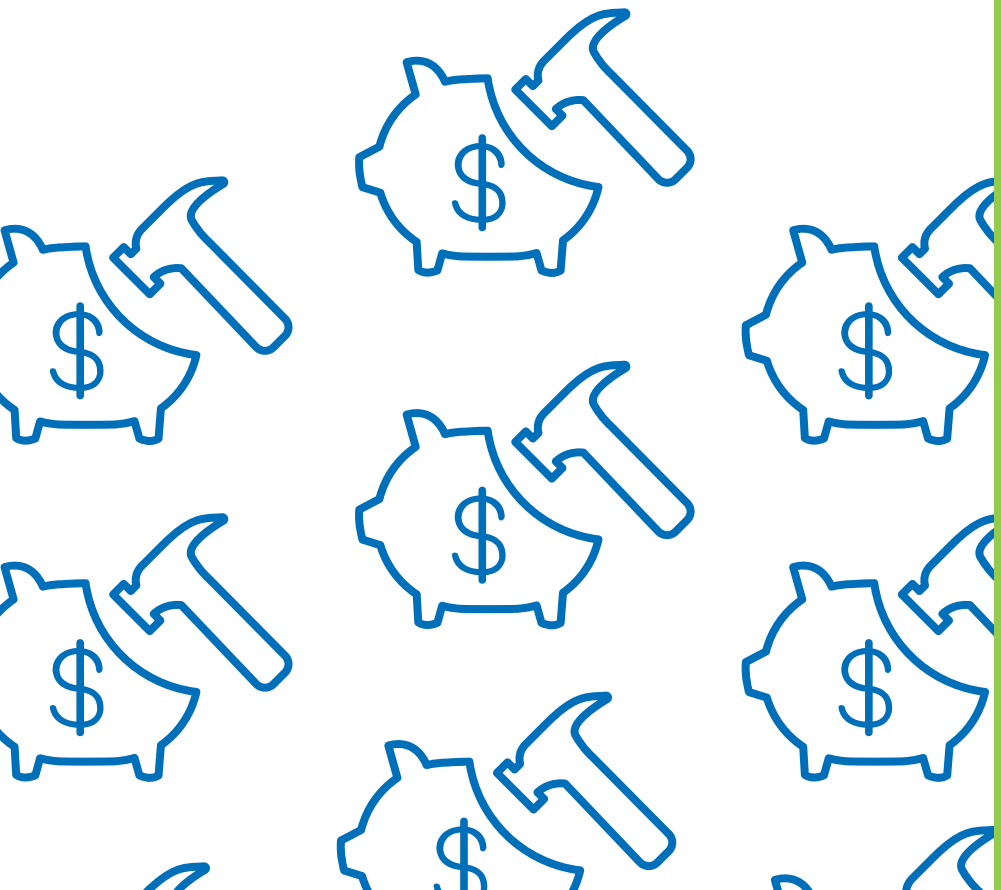
WEBROOT®
Smarter Cybersecurity™

MSP GUIDE:
IMPLEMENTING A LAYERED CYBERSECURITY STRATEGY

A single breach could put your clients

OUT OF BUSINESS



Today's threats use multiple vectors to attack, from malicious email attachments to infected web ads to phishing sites. Criminals combine a range of threat technologies, deployed in numerous stages to infect computers and networks. This blended approach increases the likelihood of success, the speed of contagion, and the severity of damage.

The only way to keep your clients safe is with a layered cybersecurity strategy that can secure users and their devices at every stage of an attack, across every possible attack vector. The following guide is designed to help MSPs develop an effective IT security program for their clients.

20 CRITICAL SECURITY CONTROLS FOR EFFECTIVE CYBER DEFENSE

The following list of security controls shows what measures organizations need to implement to achieve an effective security posture[1]. Don't be overwhelmed; most security-focused organizations already have some of these in place, even if they are not fully automated or integrated.

[1]SANS Institute. "Layered Security: Why It Works."

01 Inventory of authorized and unauthorized devices

02 Inventory of authorized and unauthorized software

03 Secure configuration for hardware and software on mobile devices, laptops, work stations and servers

04 Continuous vulnerability assessment and remediation

05 Malware defenses

06 Application software security

07 Wireless device control

08 Data recovery capability

09 Security skills assessment and appropriate training to fill gaps

10 Secure configuration for network devices such as firewalls, routers, and switches

11 Limitation and control of network ports, protocols, and services

12 Controlled use of administrative privileges

13 Boundary defense

14 Maintenance, monitoring, and analysis of audit logs

15 Controlled access based on the "need to know"

16 Account monitoring and control

17 Data loss prevention

18 Incident response and management

19 Secure network engineering

20 Penetration tests and Red Team exercises

CREATING A SECURITY PLAN THAT ACTUALLY WORKS

STEP 01

ASSESS RISK

Assessing your clients' risk allows you to jointly determine the proper security policies and procedures to put into place. To effectively assess risk, you need to examine threats, vulnerability, and assets.

THREAT ASSESSMENT

Reviewing the following four profiles with your clients will help pinpoint the most frequent or likely threats they may experience.

01

MALICIOUS INSIDER

Someone associated with your client's organization who wants to create harm, such as a disgruntled employee or contractor.

02

MALICIOUS OUTSIDER

A hacker or someone involved in industrial espionage. These are the most frequent types of threats organizations face, and the most expensive.[2]

03

ACCIDENTAL INSIDER

A client's employee or contractor who is poorly trained in the security practices. Examples include an employee who uses his birthdate as a password, and shadow IT, in which a department (such as marketing) bypasses IT to set up their own Dropbox account with a shared password.

04

NATURAL CAUSES

Companies with facilities on a flood plain, in a tornado zone, or in an area that is susceptible to wildfires or other natural disasters can be at risk for losing critical assets.

[2]Ponemon Institute. "2017 Cost of Data Breach Study." (June 2017)

VULNERABILITY ASSESSMENT

The best cybersecurity won't protect your clients if they don't address existing vulnerabilities within their organizations. Run through this checklist with your clients to determine which areas need attention.

01 Do you have a security plan in place? Who has access to it?

02 Do you have account management and access controls in place?

03 How often do you review your audit logs?

04 What are your policies for data segregation and encryption?

05 Does your organization have a Chief Information Security Officer (CISO) or someone who is dedicated to enforcing and maintaining security policies?

06 Do you give employees and contractors only enough access to do their jobs (i.e., least privilege)?

07 Do you have virus protection? How often do you update it?

08 What method do you use to dispose of sensitive data?

09 Does your company have a bring-your-own-device (BYOD) policy?

10 Does your organization have session controls in place?

11 Do you have a backup/ business continuity plan?

12 Where are your servers located? What access controls do they have?

13 Does you have a password policy for all company-issued devices?

14 What security products do you already have (e.g., firewall, intrusion detection, encryption)?

15 Have you applied all applicable security patches?

16 Are your employees and contractors trained in security best practices?

ASSET IDENTIFICATION

Many organizations are lax about maintaining an inventory of their assets, such a laptops, tablets, smartphones, and servers. Unfortunately, without updated inventory and network documentation, your clients can't effectively manage their assets, nor can they protect them. Additionally, not having an accurate inventory can pose significant problems when an attack occurs. For example, a hospital that falls victim to ransomware may have trouble locating a backup server that contains critical protected health information. Educate your clients on the importance of maintaining an accurate inventory that is categorized and rated according to their need for confidentiality, integrity, and availability.

STEP 02

DOCUMENT AN ORGANIZATION-WIDE SECURITY PLAN

Here are some baseline components for an organization-wide security plan.

01

SECURITY POLICY PROCEDURES, GUIDELINES, AND STANDARDS

This includes management controls (risk assessment, review of security controls), operational controls (personnel security, physical security), and technical controls (identification and authentication, access controls).

02

SECURITY TRAINING AND AWARENESS

Security awareness training should be conducted annually, at the very least. Email updates and other reminders can be sent throughout the year.

03

INCIDENT HANDLING

Central management and reporting of all incidents is important to understanding an organization's security posture and to coordinate a response to a potential attack.

04

COMPLIANCE REVIEWS AND ENFORCEMENT

Compliance reviews consist of annual reviews of applicable security systems and documentation including security plans, risk assessment reports, contingency plans, etc. Additionally, the a company's data may also be subject to third party compliance requirements, such as PCI for financial transactions or HIPAA for healthcare information.

STEP 03

ESTABLISH A SECURITY MANAGEMENT STRUCTURE AND CLEARLY ASSIGN SECURITY

The organization's executive management team needs to determine if they require a senior security leader, such as a CISO, and what level that person should report to the team.

STEP 04

IMPLEMENT EFFECTIVE SECURITY-RELATED PERSONNEL POLICIES

As part of their overall security strategy, companies should emphasize the following practices across all of their departments.

01 Require background checks on employees and contractors

02 Ensure personnel have completed and signed nondisclosure agreements (NDAs)

03 Enforce termination and transfer procedures including:

- **Returning equipment, ID badges, access keys, etc.**
- **Terminating user IDs and passwords**
- **Identifying nondisclosure period effectiveness**

STEP 05

MONITOR THE EFFECTIVENESS OF YOUR SECURITY PROGRAM

Your clients' security programs need to be reviewed and updated regularly in order to keep pace with today's ever-evolving cyberattack methods. You can counsel your clients to conduct regular scans of technical controls and system vulnerabilities to help stay up to date with new threats. Performing annual penetration tests can simulate the threat of someone trying to break into their organization's network and determine the effectiveness of their response procedures.

"TODAY'S ADVANCED MALWARE IS INCREASINGLY DIFFICULT TO REMOVE AND EVEN HARDER TO DETECT"

Tyler Moffitt,
Senior Threat Research Analyst, Webroot Inc.

EDUCATING THE CLIENT

When discussing cybersecurity solutions with your clients, cover the following points to get the conversation started.

CYBERCRIMINALS HAVE A VARIETY OF TOOLS AND RESOURCES AT THEIR DISPOSAL

Today's cybercriminals deploy increasingly sophisticated cyberattacks including malware, phishing, and ransomware. Research from the Webroot 2017 Threat Report found that 94% of all malware is unique to a single endpoint device, meaning most malware is polymorphic and previously unknown.[3]

Ransomware is also on the rise, with attacks such as WannaCry and NotPetya effectively shutting down global corporations, hospitals, and other institutions, or forcing them to resort to paper-based systems.

[3]Webroot Inc. "2017 Webroot Threat Report." (February 2017)

INTERNAL INCIDENTS CAN BE EVEN MORE DAMAGING THAN EXTERNAL ONES

While many companies protect themselves from external threats, internal incidents can be just as devastating, or more so. The increased mobility of an organization's data, combined with BYOD initiatives, create ample opportunities for cybercriminals. According to the Ponemon report, 52 percent of incidents involved a criminal or otherwise malicious attack. However, 24 percent of incidents were caused by negligent employees, and another 24 percent were caused by system glitches, including both IT and business process failures.[4]

[4]Ponemon Institute. "2017 Cost of Data Breach Study." (June 2017)

TRADITIONAL ANTIVIRUS PROTECTION ISN'T ENOUGH TO PROTECT AGAINST MULTI-VECTOR THREATS

Today's antivirus solutions are often designed to monitor and block malware on single channels, and can't address multi-vector attacks. They are also extremely resource-intensive. In light of the evolving threat landscape, most organizations need a cloud-based, multi-layered security defense. Such solutions leverage big data, machine learning, and collective threat analysis from customers and technology partners to identify infections as they occur, so they can be quickly neutralized.

UNDERSTANDING CYBERATTACKS

IIn addition to pointing out key events within today's threat landscape, you can also educate clients on how cyberattacks are deployed and spread. Most cyberattacks typically start with some sort of phishing attack against a user. Although random phishing attacks are relatively common, hackers often target a specific audience.

When a user falls for the phishing attack or clicks on a malicious site, the endpoint gets infected. Hackers then use these initial infections as launch points, getting deeper into the organization's systems where they can access valuable data such as admin passwords, credit card information, and protected health information (which can be even more valuable to criminals than credit card numbers).

Once they have compromised these computers, attackers may also engage in other damaging activities such as distributed denial-of-service (DDoS). In essence, the attackers intentionally "paralyze" a computer network by flooding it with data sent simultaneously from many individual computers.

CYBER SECURITY BEST PRACTICES

01

PATCHING

A typical web application can experience hundreds, even thousands, of individual attacks each year because hackers are always scanning for vulnerabilities. Patching ensures your clients' systems are up to date, which makes it more difficult for hackers to penetrate them.

02

VULNERABILITY MANAGEMENT

Regularly scanning for vulnerabilities will determine areas within your clients' systems that are outdated or require a patch. This simple, low-cost practice alone can drastically improve security.

03

LOG MONITORING

Log monitoring looks for anomalies in logs, such as privileged user abuse. This can help your clients identify threat patterns.

04

THREAT DETECTION

Threat detection includes your clients' firewalls and intrusion detection systems (IDS). A firewall is the first step to monitoring and controlling network traffic based on your clients' security rules. A good IDS can detect anything that may get through the firewall. It also uses advanced heuristics to identify traffic behavior patterns that could be malicious.

04

EFFECTIVE BACKUP SOLUTIONS

Backups are essential for remediating malicious activity and ensuring business continuity in the event of an attack. Having a regular backup solution also addresses concerns about whether your clients have ready access to the latest versions of their applications and data. This is critical for organizations that must meet certain compliance mandates, such as HIPAA or PCI-DSS.

04

ACCESS PRIVILEGE REVIEWS

Your clients should regularly review which team members have access to mission-critical data and applications. They may discover that an employee has left the organization or moved to a different department where they no longer need access. Encourage your clients to cull their lists and make sure employees have only the level of access necessary for their jobs.

BECOME AN MSP PARTNER

Webroot offers a family of services and solutions that protect users and devices no matter how or where they connect, across all the stages of a cyberattack. Our multi-vector endpoint protection, mobile protection, DNS protection, and Security Awareness Training help make businesses their most secure, and MSPs their most profitable.

To learn more about how multi-vector protection from Webroot can help you keep clients safe and become more profitable, visit www.webroot.com/MSPpartners

ABOUT WEBROOT

Webroot delivers network and endpoint security and threat intelligence services to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Our award-winning SecureAnywhere® endpoint solutions and BrightCloud® Threat Intelligence Services protect millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, Citrix, F5 Networks, Aruba, Palo Alto Networks, A10 Networks, and more, Webroot is headquartered in Colorado and operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity™ solutions at webroot.com.