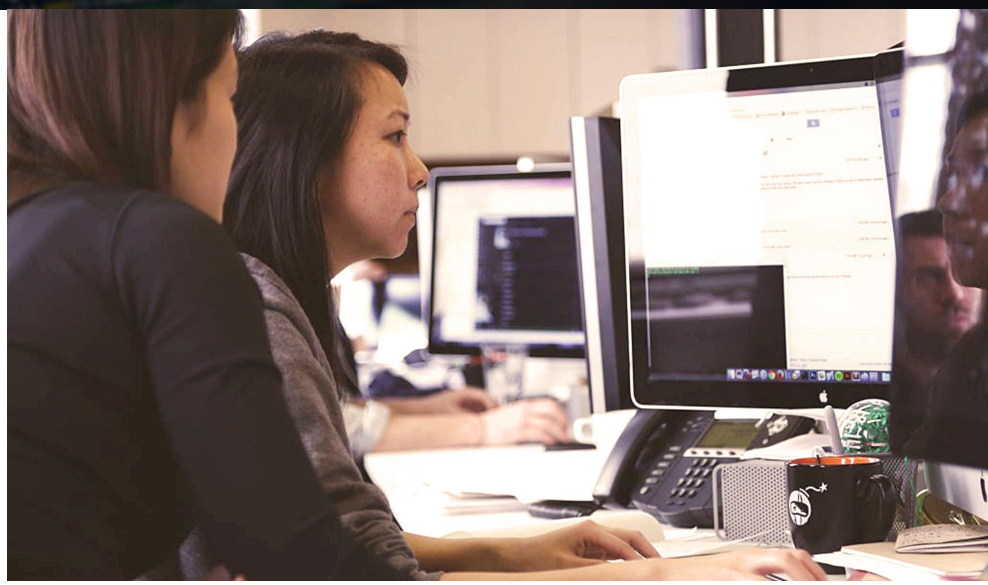
EASTWIND NETWORKS

Defense in Depth for Small and Medium Enterprises



Cyber threats often seem like far off, exotic events that don't affect the average business. The media tends to cover breaches at well-known companies, but hackers have begun to target smaller businesses at an escalating rate and SMEs are quickly becoming a primary target. The truth is that hackers know SMEs have minimal protection and are often easier to infiltrate.

The security challenge for most businesses today is balancing best practices like defense in depth with the realities of a limited IT budget and resources. Defense in depth is a cybersecurity approach based on layering protective elements to bolster security.
Traditional defense in depth layers include: data, application, endpoint, internal networks, perimeter networks, physical barriers, policies, procedures and awareness. Using this methodology, a breach in a single layer does not result in a breach of the organization.

STRAINED STAFF AND BUDGETS

Few SMEs have dedicated IT security teams or can afford the equipment to maintain the multi-layered security approach popular among enterprise and larger organizations. Hackers utilize phishing campaigns, watering holes, driveby downloads, trojans, denial of service (DoS), ransomware and other methods to breach organizations, collect and exfiltrate information to disrupt services.

IT professionals with limited security budgets need to adopt smart practices that optimize resources and bolster their protection efficiencies. Security solutions, from firewalls to intrusion prevention and detection systems, can strain budgets for most businesses.

And that's not to mention the cost of expert personnel required to manage and monitor them. Small and medium-size businesses need to find ways to provide and adapt necessary coverage, suited to fit their unique needs. Hackers depend on mistakes, vulnerabilities and unassuming users so an IT professional's job is to reduce the attack surface, educate users and implement appropriate security policies.

Here's the rundown for defense in depth elements every business needs (and can afford).

POLICIES, PROCEDURES AND AWARENESS

Start by developing cybersecurity policies. Most medium-size organizations likely have policies in place; however, to jump start this process consider any of the following resources:

- The Federal Communications Commission's Small Biz Cyber Planner tool[1]
- The Small Business Administration's Cyber Security for Small Business Course[2]
- NIST Cyber Security Framework[3]
- Center for Internet Security Critical Security Controls[4]
- US-CERT C3 Voluntary Program[5]

These resources provide the foundation for building a successful security program but each organization must balance the guidance with their own risk tolerance. While policy, procedure and technology solutions all play a role, it is also important to note that there is a burgeoning market for cyber risk insurance to transfer some of the risk. Note, that most insurance providers will evaluate your security posture before determining your policy premiums. That said, for malicious activity such as ransomware that encrypts servers, laptops and file systems, cyber risk insurance may be appealing.

Users play a large role in preventing an intrusion or breach but good habits only happen through proper education. Employees need to practice good digital hygiene like not opening email attachments from unknown senders, logging on to public Wi-Fi networks, using care in transporting data with USB storage devices and having the most updated software on all bring-your-own-device (BYOD) technology. Businesses need clear policies written by IT personnel and enforced through technology solutions and HR. These policies serve as touchstones for education to help users be part of the solution instead of the problem and as a way to enforce security monitoring on devices even while off-network.

1. fcc.gov/cyberplanner 2. sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses 3. nist.gov/cyberframework
4.cisecurity.org/critical-controls.cfm 5. us-cert.gov/ccubedvp

SECURITY SOLUTIONS

Given the understanding of defense in depth, technology solution layers range from firewalls to antivirus, intrusion detection and protection, two factor authentication, web application firewalls and more, the list goes on. You can see the difficulty in selecting and combining security solutions. How can you buy and manage all of these solutions with limited resources? Unlike large enterprises that use best of breed solutions to address many risks, for SMEs this is not possible. One approach is to consider multi-function security solutions that bundle several capabilities into a single platform. An example of this type of solution is a unified threat management solution. In this scenario, a single solution could provide firewall, antivirus, data leakage prevention, content filtering and anti-spam in one product. This reduces the organization's cost and overhead to properly manage the solution.

Unfortunately, even with all of the layers mentioned above and the right policies and solutions in place, breaches still regularly occur. For example, Yahoo, Home Depot, Target and Dropbox are all recognizable names that have been in the news recently. So what should your company do?

THE CASE FOR BREACH ANALYTICS

Investigations and responses into breaches are time consuming, costly and can potentially involve reputation risk and loss of intellectual property that can threaten your business. The average time an attacker is in your environment after a breach is 259 days. Bringing in outside cybersecurity firms to investigate breaches can run on average either $400 per hour or $10,000 per machine. Breach analytics solutions offer multifunctional attack detection capabilities coupled with incident response functions to quickly identify breaches, scope the problem and reduce attacker dwell time. They function as a system of record for all network activity accelerating investigations reducing both time and cost. Breach analytics solutions provide total visibility of your network aiding all layers of the defense in depth model. When one of the layers in the defense in depth model fails, breach analytics solutions provide the necessary information to contain, eradicate and recover from malicious activity.

PLAN FOR THE WORST

The last layer of a comprehensive defense in depth system includes planning for the possibility that all other layers fail. A disaster recovery plan ensures business continuity when disaster strikes. Having offsite backups is essential, but knowing how to recover data from them and how long it will it take is just as important. The recent ransomware attack at Hollywood Presbyterian Hospital, which took two weeks and a $17,000 ransom to resolve, was a wakeup call to many. Just a month after that attack, two Prime Healthcare Service hospitals in California confirmed they paid no ransom after being targeted with ransomware. The takeaway from both of these scenarios is that a plan needs to be in place before disaster strikes. Lockdown, isolate, eradicate and recover are the basic steps when an intrusion occurs. Each company must plan for how this will work for their unique system.

BRINGING IT ALL TOGETHER

The defense in depth mindset takes all these distinct layers into account and evolves as threats evolve. The average amount of time before a hack gets detected is dropping, but it is still measured in months, not days. No business, however small or large, can afford that kind of exposure. Setting up a comprehensive and layer-rich cybersecurity defense strategy may be the difference between survival or failure of your business.

Eastwind Networks offers the industry's only breach analytics cloud that encompasses your corporate network, off premise users, and cloud providers to provide complete visibility. Founded in 2014 and led by a team of Internet security veterans, Eastwind Networks was recently named a Founders 50 member by Dell.
For more information, please visit eastwindnetworks.com.

Watch

Collects telemetry from traditional networks, virtual environments, cloud provider-sand user data.

Hunt

Performs continuous backward and forward monitoring to identify threat actors, scope incidents, and reduce dwell time.

Analyze

Fuses multiple intelligent sources, machine learning, signatures, and anomaly detection with a fast and powerful query engine to interpret months or years of data.

Visualize

Empowers analysts to pivot and navigate complex relationships revealing previously unknown patterns

GET STARTED WITH AN EASTWIND SERVICE PROVIDER

Eastwind Networks offers an affordable option for businesses that do not have the financial resources to set-up a security stack and keep up with security changes internally. Managed Service Providers (MSP) provide businesses with technology and security support. MSPs have the expertise and resources to stay ahead of technology trends, changes and updates. Investing money in technology is necessary and expensive; therefore it is imperative that you have the proper support to maintain your security technology to continue normal business operations and focus on growth. Keep your customers, employees and partners safe from cybercrime with a MSP. MSPs reduce extra internal cost, time and effort.

TO LEARN MORE ABOUT EFFECTIVE DEFENSE IN DEPTH STRATEGY AND DISCUSS THE SPECIFIC NEEDS OF YOUR BUSINESS, TALK TO AN EASTWIND NETWORKS PARTNER: