LOCKDOWN LESSONS

Shoring up Your Network and Security Policies

Ultimately, every business wants to do what they can to best serve their clients and customers. They also want to grow successfully, increase profits, and create lasting relationships for long-term recurring revenue. But in today's cyber-climate, if you don't have a good security setup, the chances you'll get breached get higher every day. That means all the customers who trust you will have their confidence shaken—no matter how good your products or services are.

Whether you're a small- to medium-sized business or a managed service provider (MSP) who serves other organizations, strong security needs to be at the core of your business. Here a few simple security policies that will help you close security gaps and, ultimately, secure customer trust.

WEBROOT
Smarter Cybersecurity®

Enforce Strict Password Policies

Password reuse is pretty common, but it's a major security risk. For example, if a cybercriminal happens to obtain an end user's Amazon password in a phishing attack, they may attempt to use that password to access the user's other accounts. Now, what if the end user—let's call him John—also used that same password for one of the corporate systems he accesses regularly for work? In this case, the cybercriminal could gain access to John's employer's network.

It's important for system administrators to makes sure that proper rules are in place to help keep the business secure; that's where password policies come in. Password policies are a set of requirements that ensure users create strong passwords, change them regularly, and store and utilize them properly.

Pro-tips:

- Make sure passwords are complex, using special characters, numbers, caps, etc.
- Set an expiration schedule so users have to change them regularly
- Create a rule so users can't set the same password more than once
- Add restrictions to lock an account after a certain number of failed login attempts
- Enable two-factor authentication where applicable

Enforce the Access Policies based on "Least Privilege"

Regardless of your business, there's always churn. You have to on-board and off-board regularly, and employees may make lateral moves or get promoted within the company. Each time this happens, the level of access necessary for these individuals may change.

> **The principle of least privilege refers to the notion that employees should only have enough access privileges to perform the required job.**

In terms of IT, least privilege reduces the risk that an attacker could compromise a low-level user account, device, or application and gain access to critical systems or sensitive data.

You should regularly review employee access controls, permissions, and privileges, with special attention to mission-critical data, applications, and sensitive network locations. You're likely to find a lot of folks who once needed access to certain systems, files, or data repositories no longer do. Leaving these systems accessible to people who don't need them to do their jobs (or, even worse, have already left the company) is a massive security threat.

NETWORK SEGMENTATION CAN ACTUALLY HELP PROTECT YOU FROM RANSOMWARE, EVEN IF IT GETS THROUGH YOUR INITIAL DEFENSES.

Segment Your Network

Along the same lines as enforcing the least privilege principle, segmenting your networks is a step that limits the type of network access that certain users, groups, or devices may have. By dividing the network into multiple, smaller sub-networks, you can ensure that sensitive information is not shared freely, and it also helps restrict the amount of damage malware can do, if an attack successfully infiltrates a part of the network. Ransomware and other types of malware are often designed to spread quickly, so they can do as much damage as possible.

Here are a few network segmentation tips:

- Keep corporate resources separate from bring your own device (BYOD)
- Force new or unknown devices to use a guest network
- Ensure guest and WiFi networks can't access sensitive resources or data

There are a variety of non-security related benefits to this step as well. For example, these measures can boost network performance by limiting certain traffic to only the parts of the network that need to see it. You can also use network segmentation to detect and locate technical network issues more quickly. Some admins may choose to set up so-called "choke points" to funnel traffic that needs to be inspected, filtered, or otherwise controlled. And, if your business is subject to certain compliance regulations, network segmentation can help you meet them (e.g., PCI DSS requires that payment systems be separate from the rest of the network.)

To see the next-gen, predictive Webroot approach to automated endpoint threat detection and response, DNS-layer security, and security awareness training, visit www.webroot.com.

To see how Carbonite backup and disaster recovery can help you gain peace of mind with complete protection from data loss, visit www.carbonite.com.

About Webroot

Webroot, a Carbonite company, harnesses the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide endpoint protection, network protection, and security awareness training solutions purpose built for managed service providers and small businesses. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Webroot operates globally across North America, Europe, Australia and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.