LOCKDOWN LESSONS

Securing Your Business First

When you consider modern attacks, it's pretty obvious that all businesses—managed service providers (MSPs), small- to medium-sized businesses (SMBs), etc.—need a strong lineup of cyber-defense tools, not just a barebones firewall and old-fashioned antivirus. You need to protect your business first, and to do that, you have to build out a strong cybersecurity stack that can actually withstand the onslaught of modern malware.

For any business, it's crucial to remember that, as needs shift, the conversation around cybersecurity services is only going to grow. That means making sure your own business has an effective cybersecurity strategy is no longer merely nice to have; it's actually a necessary part of doing business in today's world.

By following the recommendations in this guide, you can implement cybersecurity that will effectively protect your business, and also ensure your customers stay secure.

WEBROOT
Smarter Cybersecurity®

Embrace Automated Threat Detection and Response

While the term "antivirus" has been around long enough that it gets the point across to just about anyone you talk to, it really belongs in the consumer space. When you get to the business level, even if you're still talking in terms of a small office with 10 or fewer employees, you need more. You need a solution that stops threats effectively and remediates systems automatically, so you don't have to spend time and resources (that you may or may not have) on manual virus cleanup.

You need a solution that doesn't just work to stop threats, but actually puts time back in your day.

Enter automated threat detection and response. Look for solutions that not only mention artificial intelligence (AI), and machine learning (ML), but also how they use them to automate tasks, positively impact ROI, and increase speed and efficacy. With the right technology backing its threat intelligence, a cybersecurity solution not only stops threats, but actually predicts and prevents them proactively.

Add Security at the Network Layer

A recent report on global DNS threats found that businesses experienced an average of nine or more DNS-based attacks in the last year, which is a 34% increase over the previous year's data.[1] As a result, the report reveals:

- 63% of organizations suffered application downtime
- 45% had their websites compromised
- Just over a quarter (27%) experienced business downtime as a direct consequence
- 26% of businesses lost brand equity due to DNS attacks
- The costs associated with a DNS attack went up 49%.

1 in 5 businesses lost over $1 million per DNS attack.[1]

With numbers this high, you don't even need to do the math to see how preventing DNS attacks could make all the difference to a business' success (not to mention survival). You should strongly consider investing in additional protection at the DNS layer.

Educate and Train Your End Users

The best security in the world can't protect a business if your own employees unwittingly open the door to cybercriminals by clicking a phishing link. You need to educate and empower your end users to become a strong first line of defense for your organization.

The key to achieving good results with security awareness training is in its consistency and pace. Annual and even semi-annual training is unlikely to give you the results you want because phishers change their techniques and hooks from month to month. The training needs to keep up with those changes and incorporate them into simulated phishing attacks and training courses. But the results speak for themselves.

[1] IDC. "IDC 2019 Global DNS Threat Report." (June 2019)

AFTER 12 MONTHS OF TRAINING, END USERS ARE 70% LESS LIKELY TO FALL FOR A PHISHING ATTEMPT.[2]

Back up Your Data

If your end users are the first line of defense, backup and disaster recovery is your last. In the event that a threat gets through and wreaks havoc on your networks and endpoints (for example, ransomware successfully encrypts all your client records), you need to be able to restore everything from secure backups quickly and easily, so you can keep business downtime to the absolute minimum.

Some types of ransomware and other threats can locate and encrypt files on mapped, unmapped, external, and even cloud drives. You should back up your data in at least three different places:

- Your main storage area (file server)
- Local disk backup
- Mirrors in a cloud business continuity service

In the event of a ransomware disaster, this set-up will give you the ability to mitigate any takeover of your data and almost immediately regain the full functionality of your critical IT systems. Be sure to test your backups regularly, both for security and viability, and, develop a strong disaster recovery plan so that everyone in the organization knows their role to help get systems back up and running.

When you put all of these together, they give you a strong security foundation. Not only will it keep your business safe, but it can also help MSPs develop a better-rounded offering.

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.

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.

[2] Webroot. "2019 Webroot Threat Report." (February 2019)