6 CYBERSECURITY BEST PRACTICES FOR BUSINESSES AND MSPS

Use these simple steps to prevent breaches and protect customer trust.

If you're a business or managed service provider, then you understand how critical trust is to your continued success. But when cybercriminals breach businesses—or, worse, breach MSPs to get to their clients—that crucial trust can disappear in an instant, taking your success with it.

Here are 6 simple cybersecurity best practices to help you keep your customers and reputation safe.

1. VULNERABILITY MANAGEMENT

Regularly scanning and testing for vulnerabilities will determine areas within your or your clients' systems that are outdated, require a patch, or could use other improvements.

This process is simple, low-cost, and an all-around easy win that can drastically improve security by itself. See our guide on how to perform a thorough vulnerability assessment.

2. Patching

Speaking of outdated systems and patches… In light of the OS exploits and application vulnerabilities we've all heard about in recent news, this step should go without saying. A typical application can experience hundreds, even thousands, of individual attacks each year because malicious hackers are always on the lookout for vulnerabilities.

Businesses and the MSPs who serve them should make it a priority to keep systems patched and up to date to decrease the risk of a cybercriminal exploiting outdated software or hardware to infiltrate the network. (MSPs, this applies to the systems you use in-house, too.)

3. Threat Detection

This one should also come as no surprise. In addition to effective, reliable endpoint security on every device, threat detection includes 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 and block anything that may get through the firewall, and will also use advanced heuristics to identify traffic behavior patterns that could be malicious.

4. Log Monitoring

Always examine reports and monitor logs to look for anomalies, such as privileged user abuse. This can help you identify threat patterns and close security gaps.

Depending on the size of the business and the number of devices and networks to be monitored, you may want to use a security information and event management (SIEM) solution or a similar tool to help you sift through the data to prioritize which items need attention and when.

5. Effective Back-up 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 you and your customers have ready access to the latest versions of business applications and data.

This is especially critical for organizations that must meet certain compliance mandates, such as HIPAA or PCI-DSS.

6. Access Privilege Reviews

In every business, there's churn. Between on-boarding, off-boarding, and lateral moves within an organization, you should regularly review which team members have access to mission-critical data, applications, and sensitive network locations. You may discover a number of employees who once required access to certain systems or files no longer do. Leaving those systems open to folks who don't really need them (or, worse, have left the company!) can be a major security risk.

Cull your lists and do regular audits to make sure employees' access is based on "need to know," i.e. they have only the level of access necessary for them to do their jobs.

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.