Quorum®

The Top 4 Security Threats of 2021

How to protect your organization

contents

Quorum

2020 saw one of the biggest single-year surges in history for IT security threats. More importantly, the factors that contributed to this surge — including the rise of remote working — are here to stay.

A report released in early 2021 by IT security firm Proofpoint highlights the magnitude of the threat for businesses worldwide. This report estimates that nearly two-thirds of businesses globally have seen an increase in targeted cyberattacks since they switched to widespread remote work.

As security threats increase, IT leaders and their teams must up their game accordingly. This means a few things:

- Being aware of the range of threats that exist today
- Prioritizing the threats that are most common and that have the potential to be the most damaging and costly
- Having the right solutions in place to deal with worst-case scenarios like data and/or security breaches

In this guide, we'll discuss the four biggest IT security threats businesses face in 2021, and tell you what you can do today to ensure your organization is protected.

1. Ransomware

According to a report by cybersecurity firm Deep Instinct, ransomware attacks increased by 435% in 2020 compared to 2019. And according to IBM Security's X-Force, ransomware was the leading threat in 2020, making up nearly a quarter of all attacks.

When successful, these attacks are very costly for businesses. As of November 2020, the average payout for a ransomware attack had grown to nearly $234,000 per event.

If that isn't enough to convince you of the importance of protecting your business against ransomware, consider this. In the future, ransomware is only expected to get better at evading malware identification due to the use of increasingly sophisticated AI.

No matter what industry your business works in, ransomware needs to be at or near the top of your list of threats.

What You Can Do

Ransomware can (and does) strike through many different avenues. The most common vulnerability is human error, often exploited through the use of social engineering attacks (we'll discuss social engineering in a later section).

That's not to say that basic security measures are ineffective. Ensuring that all computers and mobile devices are regularly updated and patched is important as a first line of defense.

However, since ransomware most often exploits human behavior, no system is ever completely safe, no matter how secure.

That's why the most critical element in preventing financial or data loss from ransomware is to have a bulletproof backup system. One that can deliver fast, easy and reliable restoration of all of your critical systems — so that you're not forced to fork over the cash to get your business up and running again.

2. Exploitation of Sysadmin Accounts and Tools

There are two basic types of sysadmin threats: internal and external.

Internal threats refer to intentional misuse by a system administrator. While these are less common, they are by no means rare. There have been some high-profile cases of system administrators getting away with misuse of account credentials for years before being caught — sometimes costing their companies hundreds of thousands of dollars.

By their very nature, internal threats are harder to prevent or detect. Still, there are some best practices you can adopt to limit your risk, which we discuss in the *What You Can Do* section below.

External threats refer to attempts by outside actors to either: 1) steal sysadmin account credentials and gain access to sensitive data and/or system control, or 2) exploit commonly used sysadmin tools to execute or plan a security breach.

Sysadmin tools are some of the most commonly targeted business software applications for hackers. In fact, according to a report by Positive Technologies, more than 50% of threat groups leverage publicly available penetration testing and/or sysadmin tools to develop attack strategies.

What You Can Do

When it comes to internal threats, separating duties is critical. This limits the amount of power and access any single system administrator has.

To protect your sysadmin accounts against external threats, use multi-factor authentication and maintain strong password management practices. Never allow system administrators to use easy-to-guess passwords or to reuse passwords in multiple places.

Additionally, make sure your physical systems (e.g., in-house servers) are stored in a place with restricted access to prevent in-person security breaches.

3. Remote Working

Remote work is the new normal for organizations across industries. According to Gartner, 64% of employees are now able to work from home, and 40% are actively doing so.

More remote workers mean more data routinely being sent across network boundaries — and data security outside of your business' home network is much more challenging to secure.

Additionally, VPNs, RDPs and all other network access tools create another point (or multiple points) of potential vulnerability, increasing the "surface area" where attacks can occur.

What You Can Do

Fundamental, company-wide security best practices are even more important when a portion of your workforce is remote. These include:

- Strong passwords
- Periodic password changes for all users
- Multi-factor authentication
- Ensuring proper access based on role/ responsibility
- Requiring remote workers to keep computers and mobile devices updated
- Ongoing education and reminders about threats and potentially dangerous behaviors

4. Social Engineering

Social engineering attacks are the most challenging to prevent because they exploit user behavior to gain access.

Even the most secure IT system can be breached if an employee makes a momentary bad decision in clicking on a suspicious link, entering credentials into a phony website, or downloading a document loaded with malware.

Social engineering attacks take many forms, including phishing, smishing (sms/ text-based phishing scams) pdf scams and even in-person attacks like USB baiting — in which an attacker leaves a malware-laden usb drive out in plain view in the hopes that someone will connect it to a computer in order to identify the owner.

What You Can Do

Social engineering attacks are particularly frustrating for IT departments because no automated security measure can prevent them. They're entirely up to user vigilance.

Therefore, an aggressive, continuous training and communication program is the top priority.

Social engineering attacks occasionally involve unauthorized personnel gaining physical access to your offices and/or server locations. Combat this by creating and enforcing clear policies and procedures for managing and authenticating physical access to your site.

Prevention is Important, But It's Not Enough

By taking the steps outlined above, you can reduce the likelihood that your business will be the victim of a security breach.

However, even the most secure systems are never bulletproof.

For that reason, a fast, efficient and easy-to-operate disaster recovery system needs to be a priority for every organization.

Quorum provides best-in-class high availability and disaster recovery solutions for businesses of all sizes. Our true one-click solution offers continuous backup, automated testing, and a fast and ultra-simple process that gets your most vital systems back up and running in seconds.

Visit our website today to learn more about why Quorum's onQ disaster recovery system is the solution of choice for business worldwide.

Quorum: The Leader in Disaster Recovery

Quorum provides the fastest, most reliable, and easiest-to-use high availability and disaster recovery systems on the market. Our industry-leading technology is built to deliver the ultimate in flexibility, performance and value. With Quorum, you no longer have to choose between cloud vs. local or cost vs. performance. **Visit our website** to learn why Quorum is the world leader in HA and DR solutions.

Contact Quorum Phone: 877-997-8678 Email: ussales@quorum.com