5-Minute Security Brief: What you Need to Know About Ransomware

Ransomware isn't something that happens to someone else

By the time you finish reading this paragraph, another business will be the victim of ransomware. Experts estimate that, this year, a new ransomware attack will occur every 11-14 seconds around the world.[1] For organizations in the public sector, where ransomware payments can be up to 10x higher than in the private sector[2], that fact will hit especially close to home. In the state of Georgia, for example, recent ransomware attacks on Jackson County and the City of Atlanta cost taxpayers hundreds of thousands of dollars in ransom payments and millions of dollars in recovery costs. Unfortunately, numbers like these virtually ensure that ransomware attacks will grow. So long as it's profitable and effective, cyber criminals will continue to target government organizations, enterprises and even small businesses with ransomware.

A ransomware attack happens every

11-14

seconds

The rapid rise in ransomware isn't just a matter of higher ransom payments. It has become increasingly easy for cyber criminals to launch ransomware attacks through the proliferation of mobile devices—including personal devices and shadow IT applications that are part of the Bring Your Own Device (BYOD) trend—and the growing number of connected devices brought by the Internet of Things (IoT). The adoption of smart devices and capabilities is seen as core to digital transformation and is increasingly part of technology strategies across industries. **Gartner forecasts 20.4 billion connected things will be in use worldwide by 2020.**

The growing prevalence of embedded connectivity also means a growing attack surface. Security and IT leaders are simply overwhelmed with the number of endpoints, applications and databases that need to be monitored and protected. Cyber criminals have become experts in exploiting the weakest link in the security chain and what's in the balance is significant. Some potential IoT ransomware scenarios? A contractor sends data from her personal smartphone over a public Wi-Fi network and exposes all internal systems. A medical facility loses control of connected medical devices that regulate pacemakers, insulin injections or electronic health records (EHR) across the organization. Robotics within manufacturing, a tablet directing logistics, voting machines, a thermostat, a lightbulb, if it uses the internet for functionality, it is at risk for a ransomware attack.

There's no time to think about ransomware protection *after* an attack

Once a ransomware attack is initiated, decision makers may have only a matter of hours before deciding whether or not to pay the ransom. As IT professionals scramble to assess the extent of their vulnerability, including what data has been compromised and whether viable data backups exist, executives have to weigh the cost of paying the ransom against the cost of losing data and/or operational capabilities. Their first consideration is usually the data itself—specifically, whether the data being held for ransom is mission-critical and when the last secure data backup was performed. In most cases, however, the true cost of the attack comes down to operational considerations: lost productivity, lost revenue and, perhaps most importantly, lost trust from customers and constituents. The cost of downtime during a ransomware attack often exceeds the ransom amount itself, a strategy that cybercriminals use to their advantage time and again.

In very few cases are organizations able to remove ransomware. At best, they can hope to mitigate its effects through air-gapped backup systems, network microsegmentation and other preventive techniques. Most organizations, however, find themselves unprepared for a ransomware attack. In the days and weeks that follow, much handwringing ensues as IT and security teams wonder what they could have done to better protect their data. Sadly, in many instances, the ransomware attack was the result of something that could have been easily avoided, such as a software application that wasn't updated or a phishing email that slipped through the network.

What can we do to prevent ransomware?

There isn't any one thing you can do to protect your organization against ransomware. Instead, a multi-layered security solution is required to protect data at rest, in motion, on mobile devices, in the cloud and anywhere that data resides. One weak link in your data protection chain is all cybercriminals need to penetrate your defense. One phishing email accidentally clicked can open the door to thousands of dollars in damages. In a world where 3.2 billion fake emails are sent every day[3], the odds aren't in your favor.

So what should you do to strengthen your defenses against ransomware?

1. **Encrypt your data.** In your data center, in the cloud, on your endpoints and devices (laptops, smartphones, connected sensors, IoT, etc.) and especially while data is in motion over any network.
2. **Block bad actors from getting into your network.** This can be done through secure firewalls, identity and access management (IAM) as well as strong security policies that include blacklisting of malicious and suspicious IP addresses.
3. **Secure remote access to your network through virtual private network (VPN) encryption.** With more organizations allowing remote and mobile workers to access business applications and data from home or other offsite locations, secure VPN connectivity is critical to preventing "man-in-the-middle" attacks.

4. **Keep up to date with the latest threat intelligence.** New attacks are constantly being spawned and it's critical for any organization to not only share threat intel in real time across every branch/office but also share this information with other trusted organizations. Think of it as standing united against ransomware.
5. **Practice good secure hygiene.** This means educating employees on how to spot phishing emails, updating passwords on a regular basis, backing up data frequently and using encrypted communications over unsecure networks such as public Wi-Fi hotspots.

Privafy can help protect you against ransomware

Privafy's cloud-based security-as-a-service is designed to help protect businesses and organizations of all sizes against cyberattacks, including ransomware, data breaches and other malware-based attacks. As part of a broader security solution, Privafy can help prevent ransomware by delivering essential security features consistently across your entire organization. Developed by security experts, Privafy combines advanced, patented technology with unparalleled simplicity for a complete security solution that can be deployed anywhere in minutes.

The Privafy solution features:

- **Absolute Encryption™** with automatically and dynamically generated encryption keys for greater protection of data-in-motion
- **Impervious Firewall™** technology protects your network perimeter from unauthorized entry
- **Endpoint Identity Protection** provides banking-grade security for all network, cloud and mobile endpoints, using a clone-proof, trusted root of authority
- **Deep Content Inspection** of incoming and outgoing traffic to block malware from getting in and stop sensitive data from getting out due to a data breach
- **Always-on, Secure IoT Connectivity** to protect connected devices against compromise, attack or infiltration
- **Non-Degrading Performance** ensures more security never comes at the cost of degraded network performance
- **Ultra-High Service Availability** protects your data even during network failures and cloud outages
- **Easy-to-Use Monitoring and Alerts** shows threats detected, attacks blocked and important security alerts in real time
- **AI-Driven Threat Detection** featuring self-learning capabilities that provide "smarter" security over time, including detection of evolving ransomware variants
- **Shared Threat Intelligence** leverages aggregated intelligence from Privafy's global security network and delivers real-time updates to every branch/office and every endpoint, eliminating weak links in your security chain.

What would you pay to avoid cyberattacks?

The cost of cybersecurity has grown with the rise in cyberattacks. Even a small organization can spend tens of thousands of dollars per year on hardware firewalls, intrusion prevention/detection systems, IDP/IDS, antivirus software licenses, threat monitoring tools—and, of course, the security experts required to manage them all. With Privafy's cloud-based security platform, you can get all that protection and more for dollars per day. No expensive hardware needed, no on-staff security expertise required; just simple, strong security that serves as a protective shield around your data and your employees as they move, anywhere, on any device.

With looming legislation that would place more government organizations in charge of their own security—including the responsibility for ransomware payments and cybersecurity insurance—now is the right time to be thinking about ransomware. Ask Privafy how we can help secure your organization against cyberattacks with our complete data-in-motion security platform. To learn more, visit us online at privafy.com.

Sources
1. Morgan, Steve, "Global ransomware damage costs predicted to hit $20 billion (USD) by 2021," Cybercrime Magazine, October 21, 2019 (Last accessed February 6, 2020), https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/.
2. Freed, Benjamin, "Ransomware hits everywhere, but governments pay 10 times more," Statescoop.com, July 16, 2019 (Last accessed February 6, 2020), https://statescoop.com/ransomware-local-government-pays-10-times-more/.
3. Spadafora, Anthony, "One trillion phishing emails sent every year," techradar.com, June 12, 2019 (Last accessed February 6, 2020), https://www.techradar.com/news/one-trillion-phishing-emails-sent-every-year.

About Privafy

For business leaders in charge of sensitive information, Privafy's security-as-a-service application has reimagined how to protect Data-in-Motion. The company's cloud-native technology integrates all the functionality of traditional point solutions to provide comprehensive protection as data traverses between locations, clouds, mobile devices, and the IoT. Deployed in minutes, Privafy is the only solution that works seamlessly with existing infrastructure to protect organizations of all sizes against today's most damaging data-centric attacks, all while disrupting the cost associated with complex, archaic network solutions. For more information, visit at privafy.com and follow Privafy on Twitter and LinkedIn.

Privafy, Inc.
2 Burlington Woods Drive
Burlington, MA 01803

www.privafy.com