PUBLICATION

Happy Hack-tober! Don't be Scared: How to Protect Your Business from RaaS Threats

Authors: Matthew George White
October 01, 2024

October is here, and as we prepare for pumpkin spice lattes, fall sweaters, and scary decorations, there's one thing your business can't afford to ignore this month: cybersecurity. Welcome to Hack-tober, or as it's officially known, Cybersecurity Awareness Month – a great time for your business to review policies and procedures to mitigate against cyberattacks.

One trend that's making headlines: Ransomware-as-a-Service (RaaS). No, that's not the name of a heavy metal band. It's a thriving underground business model that your business should account for while making cybersecurity preparations. In this alert, you will learn more about RaaS attacks and what you can do to protect your business.

Ransomware-as-a-Service

RaaS allows bad actors to "subscribe" to ransomware software and use it to launch attacks without needing advanced technical skills. Picture a group of cybercriminals sitting around, discussing a "business partnership," but instead of selling cookies or vacuum cleaners, they're selling data-scrambling, system-locking malware to the highest bidder.

This isn't your classic "guy in a hoodie in a dark basement" stereotype anymore. It's sophisticated. It's scalable. And worst of all, it's accessible. Anyone with a credit card and internet access can become a ransomware kingpin, turning the world of cybercrime into a subscription service.

Remember when Netflix used to send DVDs to your mailbox? With RaaS, the only thing sent to your business might be ransom demands. But wait, there's more! Hackers are no longer satisfied with a simple ransom. Welcome to the era of **double** and **triple extortion attacks**. Think of it as the "premium subscription" to ransomware, where hackers hit you with the full package of terror.

In a **double extortion** attack, bad actors don't just lock your data and demand payment to unlock it. They also **steal your data** and threaten to leak it publicly or sell it to other cybercriminals if you don't pay. And because hackers are always looking to innovate (just like your favorite streaming services), some are upping the ante with **triple extortion**. Here, after locking and stealing your data, they start harassing your **customers, partners, spouses, and/or suppliers,** demanding a ransom from them too. Suddenly, everyone in your business ecosystem is receiving ransom demands.

Why Your Business Should Care

Small to medium-sized businesses often think, "We're too small to be a target," or "Hackers are only after big fish." In reality, small to medium-sized businesses are prime targets for these attacks because hackers know these businesses often lack the cybersecurity resources of larger enterprises. Recent studies have shown that RaaS operators are casting a wide net. According to Coveware's Q2 2024 Quarterly Report, approximately 35 percent of ransomware victims were companies with 11 to 100 employees; 31 percent were companies with 101 to 1,000 employees; and 20 percent were companies with 1,001 to 10,000 employees.

Let's talk consequences:

- **Lost Revenue**: A ransomware attack can paralyze operations, cutting off cash flow fast.
- **Reputation Damage**: Customers don't want to hand over their credit card info to a business that's been hacked. A breach can turn loyal customers into a ghost town.
- **Legal Liabilities**: The recent proliferation of privacy laws like the California Consumer Privacy Act (CCPA) aren't just suggestions, they're enforceable. Failing to protect sensitive information can lead to fines long after the breach is resolved. Add to these risks the flood of data breach class-action litigation, and you are facing the potential of financial and legal troubles.

How to Protect Your Business

As cyber threats loom large for the foreseeable future, it's important to fortify your business against these threats. The following are some best practices that will help mitigate risks from cyber criminals. However, no single solution fits all. For a full review and tailored cybersecurity advice, reach out to legal counsel to assist in crafting policies and procedures.

1. **Backup Like Your Business Depends on It (*Because It Does*)**: Invest in regular, secure, (air gapped), and tested backups. That way, if you're attacked, you potentially won't have to pay the ransom. You can restore your system from the backup like hitting "undo" on a bad decision. It's a simple precaution that works.
2. **Educate Employees**: Studies show that most ransomware attacks start with phishing emails, meaning someone in your company accidentally let the bad guy in. Regularly train your employees to spot phishing attempts and maintain good security hygiene.
3. **Multi-Factor Authentication (MFA):** Strong passwords are great, but why stop there? Add another layer of security with MFA. It's like deadbolting your doors. Even if someone has the keys, they're not getting in without a second form of ID.
4. **Patch, Patch, Patch**: Think of software patches as the digital equivalent of replacing the batteries in your alarm system. When your systems are up to date, it's harder for hackers to sneak in through vulnerabilities. Neglecting to patch your systems is like leaving your front door open.
5. **Have an Incident Response Plan**: No one plans to get attacked, but you should still have a plan for what happens if you do. It's always better to be over-prepared than caught off guard.

The Bottom Line: Don't Be Afraid, Be Prepared

Don't let ransomware make your business its next victim. Take the time to review your cybersecurity measures, train your employees, and test your response plans. And if all else fails and ransomware comes knocking, we're here to help. With the right combination of technology, preparedness, and legal support, we'll make sure your business comes out of any attack stronger.

Cyber threats don't take a holiday, and your business can't afford to either. Whether you have questions about your current cybersecurity setup, want a second pair of eyes on your privacy programs, or just want to make sure you're prepared for the latest threats (like ransomware), we're here to help. Contact the author – Matt White, or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team, and we'll guide you through your next steps. Afterall, when it comes to cybersecurity, an ounce of prevention is worth a pound of "I told you so."

Stay safe and happy Hack-tober!