WHITE PAPER

SMBs: 4 Ways to Stay Off the Ransomware Hit List

Ransomware is an industry of its own, complete with an array of black-market ransomware-as-a-service products and an underground criminal ecosystem, as discussed in the first of a six-episode video series from OpenText focused on ransomware. Staying out of the crosshairs, or at least swiftly rebounding after an attack, is now a top business imperative.

That can be easier said than done, however. Like all earlier forms of profitable crimes, cyberattacks have gone big-time. “Ransomware is a business model with huge scale and significant returns on investment for the bad guys,” says Tyler Moffitt, senior threat research analyst at OpenText Security Solutions.

That business model has proven to be highly lucrative. IDC reports that the average ransom payment was “almost a quarter million dollars.”

Such a high payoff on a single attack means that the target was large and rich. But although it’s true that attacks on the biggest companies hog the headlines, smaller companies are also getting hit regularly.

- According to a Ransomware Task Force report, “Businesses with fewer than 500 employees were hit by 70% of the attacks in 2021.”
- According to a Cybersecurity & Infrastructure Security Agency (CISA) report, “Ransomware groups suffered disruptions from U.S. authorities in mid-2021. Subsequently, the FBI observed some ransomware threat actors redirecting ransomware efforts away from ‘big-game’ and toward mid-sized victims to reduce scrutiny.”

Attacks on smaller businesses hardly ever make the news, but companies of all sizes are targeted every day. Cyberattackers might spend weeks — or, in some cases, only days — casing a target to determine how much ransom to charge for the return of its own data. What follows are four ways that you can protect your company.

opentext™ | Cybersecurity

SPONSORED CONTENT
CSO

1. Check your business vulnerabilities

Know your threat vectors: What and where are the vulnerabilities inside your organization? You're not only checking to see if all the doors are locked but if key holders are securing the keys too.

"When people think about ransomware, they think it's only a cybersecurity issue. They are not considering that most threat vectors come through humans," says Shawnee Delaney, a former clandestine ops officer with the U.S. Defense Intelligence Agency and an insider threat subject matter expert. Delaney is a featured contributor in the *Ransomware 2023* video series.

The biggest thing that should be considered under business vulnerabilities: access control. This entails making sure no employees have more access than they should, so if an employee falls for a phishing attempt and is compromised, it doesn't result in the whole company being compromised.

2. Train and protect against social engineering

Social engineering is how many organizations are compromised. By tapping into the wealth of knowledge gleaned from social media, attackers can appear legitimate. For example, bad actors can learn an organization's management hierarchy and details about a manager or executive that can then be used in a phishing email to fool an employee into doing an attacker's bidding.

"Email security is your first line of defense in a layered protection system," says Moffitt. "That's going to literally block, detect, and filter out 99% of the malicious emails that would come in. It would be able to tell through artificial intelligence and machine learning that this is a phishing email and prevent it from even making it into the employee's inbox."

Mandatory security awareness training (SAT) is another line of defense against phishing. Incorporating simulations to help identify phishing gives employees real-world practice, and conducting them every three to six months provides measurements on training effectiveness.

3. Guard against backup encryption

Many ransomware victims are dismayed to learn that their carefully built backup-and-recovery plan has also been compromised in an attack.

Obviously, something more in the way of recovery tactics is needed. Consider keeping multiple copies of the backup in different domains. For example, one copy local and another in the cloud. Likewise, consider backup solutions that do not allow an attacker to rewrite, encrypt, or modify previous backups. "These and many other measures you could take will help you achieve immutability: keeping a history of restore points and backups that cannot be compromised so you have the means to access and restore from a good copy of an earlier snapshot," says Moffitt.

4. Look for layered data protection

There is no panacea for the ransomware onslaught. Big or small, all businesses are best protected by layers of security measures. That way an attack might get through one or more but usually not *all* the protective layers. For example, if an organization already has email and endpoint security, add in security training for employees. If DNS protection already exists, add (and regularly test) a backup and recovery component.

"A layered security approach comprises multiple instances of redundancies right to where the backups are at the very bottom. Aim to stop the attack before the bad actors get to the backups, the last line of defense," says Moffitt.

> Big or small, all businesses are best protected by layers of security measures.

In addition, the layers themselves must always be revised and updated to protect against emerging threats. “You’re going to be infected. Not a question of if, it’s a question of when. Keep your guard up and remember that the more layers in your security posture, the better equipped you’ll be to defend against and recover from an attack,” says Moffitt.

The bottom line

Ransomware is now a billion-dollar industry. Attacks against small and midsize businesses are proving more profitable in the aggregate than they used to be. As further enticement, cybercriminals are aware that smaller businesses usually don’t have sufficient defenses or adequate training to thwart an attack, making them a deliciously ripe target. Protecting your company on the four key fronts outlined above is essential.

➜ **Watch *Ransomware 2023* to learn more.** Look for Episode 2 to find out more about your adversaries and how they think and work.