greenPROFIT

Features

4/1/2022

Doubling Down on Ransomware Protection

Joe Dysart

As the threat of ransomware has reached new heights in 2022, many businesses are doubling-down on their defense against the scourge—making sure they've done everything they can to avoid becoming a victim.

Many owners of even the smallest green business realize they're prime targets for these hackers, who see small businesses as generally easy to penetrate, plunder and fool.

"We have an extensive firewall system we use," says Leigh Geschwill, owner of F&B Farms & Nursery in Woodburn, Oregon.

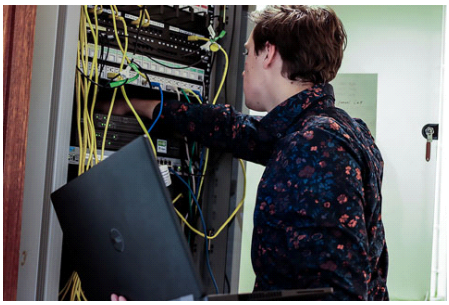
Stephen V. Mecke, CIO of Lucas Greenhouses in Monroeville, New Jersey, said that ransomware is "an extreme threat to both the private and public sectors." The impact has been so widespread that the federal government has taken steps in releasing M-22-09 (tinyurl.com/ransomwareplan), which is the federal government's own game plan for defending against ransomware and other cyberattacks.

Indeed, successful ransomware attacks across the U.S. have proven so visceral, they've triggered an executive order from President Joe Biden, nudging all U.S. businesses to get serious about ransomware protection. Said Biden, the order "calls for federal agencies to work more closely with the private sector to share information, strengthen cybersecurity practices and deploy technologies that increase reliance against cyberattacks.

"It outlines innovative ways the government will drive to deliver security and software—using federal buying power to jumpstart the market and improve the products that all Americans use."

Why You Need to Care

During 2021 alone, businesses across the U.S. reeled from successful ransomware attacks, including attacks against SolarWinds, a commonly used IT management software program; the ransomware disruption of service on the Colonial Pipeline, the largest conduit of refined oil products in the U.S.; and the ransomware seizure of computer files of the Washington, D.C. Metropolitan Police Department.



Pictured: Thirty-seven percent of organizations across the globe have experienced some sort of ransomware attack of late.

Still other ransomware takedowns include a takeover of computer files at goliath meatpacking company JBS Foods, as well as at the National Basketball Association.

Granted, authorities have occasionally gotten lucky against ransomware hackers. Excellent cyber forensic work by the U.S. Department of Justice, for example, clawed back $2.3 million in Bitcoin that the Colonial Pipeline paid to ransomware hackers to help get its computer network up-and-running again.

“Following the money remains one of the most basic, yet powerful, tools we have,” says Lisa O. Monaco, U.S. Deputy Attorney General. “We will continue to target the entire ransomware ecosystem to disrupt and deter these attacks.”

Even so, hackers more often than not get away with their exploits, extorting hundreds of thousands of businesses across the globe each year and disrupting the day-to-day operations of each.

Why it May Not Be Wise to Pay

Overall, 37% of organizations across the world have experienced some sort of ransomware attack between May 2020 through April 2021, according to a study from cybersecurity firm Sophos, “The State of Ransomware 2021.” Based on that survey of 5,400 IT managers at mid-sized organizations across 30 countries, the study also found that the average ransom paid to recover data from a ransomware attack was $170,404 USD.

Not surprisingly, many of the criminals behind those successful ransomware attacks kissed-off promises to restore computer files once ransoms were paid, according to the study. Specifically, on average, victimized businesses in the study that paid ransoms only got back 65% of their data. And only 8% of businesses forking over money to hackers were able to retrieve all of their files, according to the Sophos study.

Equally vexing for the victim organizations was the cost to day-to-day business. The average cost to restore the impact of a successful ransomware attack on a mid-size business—taking into account downtime, lost wages, device cost, network cost, lost sales and ransomware paid—was $185
million.

Plus, hackers have increasingly exploited a new wrinkle in their ransomware schemes during the past year, threatening—and often making good on threats—to publish sensitive data found in business files on the Dark Web if a victim business refuses to pay a ransom. Granted, smaller green businesses hit by ransomware are most likely going to see a much smaller impact on their bottom line than what’s being experienced at mid-level and large-sized competitors.

But even with the smallest business, a ransomware shutdown smarts, grinding its revenue stream to a halt and running the owner ragged trying to find a way to get computers up and running again. That’s why it’s imperative to start putting together a plan to handle and mitigate ransomware and similar cybersecurity threats, which many believe should include comprehensive cybersecurity insurance.

What You Can Do

In the early days of the web, businesses looking to buy insurance against cyberattacks used to focus mostly on just protecting against data breaches. But these days, insurance coverage goes much further, providing protection against the full ramifications of an attack, including data restoration, dealing with demands for ransom and similar

extortion, as well as fully restoring network security.

“Initially, businesses were covered for free under insurance for these occurrences,” notes Stephen at Lucas Greenhouses. “But now the landscape has changed to the point of cyber liability insurance being an expensive need to have—if you even qualify.”

Once you’re insured, you’ll also want to be sure you have a plan in place designed by your computer expert to safeguard against hackers, including multiple copies of your company’s data. And you’ll want to have an “incident plan” in place designed to handle all the fallout you’ll experience should you get hit by ransomware, including restoration of all computing services, notifying customers and suppliers of the breach and notifying governmental authorities.

Without such a plan, you’ll most likely be caught flat-footed, struggling to deal with a swirl of chaos that might force you to make quick decisions you’ll later regret. But perhaps most important in safeguarding your business against a hacker breach is ensuring your employees are brought up-to-speed on all the ways hackers are trying to trick them into clicking on links, revealing IDs and/or passwords or otherwise providing access to the company network that can—and often does—result in devastation.

Stephen advises: “Train your end users as they are the weakest link in the system.”

Resources Available to Help

Fortunately, the guys and gals in the white hats have been busy strengthening software designed to thwart ransomware attacks. Here’s a representative sampling of that software for you to check out, all highly rated and all available at entry level prices:

• **Bitdefender Antivirus Plus**, starts at $23.99/year: A player in the anti-ransomware space for a number of years now, Bitdefender Plus offers many layers of anti-ransomware protection, along with myriad other security features.

The software is designed to eliminate known ransomware on the spot. Plus, it also will watch for unexpected behaviors on your PC or network that indicate ransomware activity, such as a sudden, wholesale change in the names of files or the extension names of files.

In a phrase, Bitdefender backs up all your files at the first whiff of what it determines may be a ransomware attack beginning to deploy and then restores the files after the attack has been fully neutralized.

• **ZoneAlarm by Checkpoint**, $39.95/year: This is another highly rated anti-ransomware package that erases all vestiges of ransomware on your computer system once detected.

It embeds “bait” files on your computer network, designed to lure ransomware into changing those files first, setting off alarms and enabling ZoneAlarm to neutralize the attack before it spreads to actual company files.

Plus, ZoneAlarm can repair files after a ransomware attack, if possible.

• **Kaspersky Security Cloud**—Free: It’s hard to argue with free. So if you’re looking for instant peace of mind today, this one may be your ticket.

Kaspersky is designed to protect against two types of ransomware: The first encrypts your files, making them unusable to you. The second is ransomware that encrypts your entire hard disk, making the entire computing device unusable.

Kaspersky can also neutralize ransomware that locks up your computer screen. And it offers monitoring and auto-

neutralization of typical ransomware behaviors, like wholesale renaming of files and/or file extensions.

Other features include Idle Scan, which monitors resources like system memory when you're not using your computer. And there's a rootkit scan function, which helps betray ransomware activity designed to elude typical monitoring of Windows and typical monitoring used by everyday anti-virus software.

• **Sophos Home Premium**, starts at $44.99/year: This program is a lite version of a more robust version of anti-ransomware protection that Sophos offers to enterprise-level businesses.

Sophos is designed to plug known security holes in commonly used software. Plus, it offers download reputation analysis on programs that you're thinking of downloading that may have a bad reputation.

Sophos could do the trick for a small business that decides enterprise-level protection isn't necessary, especially since this lite version enables you to remotely safeguard, monitor and manage the software on up to 10 remote computers.

One caveat: Novice users may face a bit of a learning curve before they can use Sophos' advanced features.

• **NeuShield Data Sentinel**, starts at $23.99/year: NeuShield is the only candidate in this pack that doesn't offer ransomware protection.

Instead, NeuShield is an after-the-fact ransomware product, which offers users one-click restoration of files encrypted by ransomware, if possible.

Essentially, NeuShield isn't a panacea against a ransomware attack, but giving it a whirl after your business has been taken down by ransomware is well worth the price of entry.

Users install NeuShield on their computers before an attack occurs. That enables the software to "virtualize" any changes to the files on your system. Theoretically, virtualized files cannot be corrupted by a ransomware attack, given that they're not fully operational files in a virtualized state. Users of NeuShield regularly decide when to approve changes in virtualized files, which make those files operational once again.

It's a powerful way to put a buffer on any files in your system that undergo changes, including changes ransomware is seeking to make to your files. **GP**

Joe Dysart is an Internet speaker and business consultant based in Manhattan. He can be reached by email at joe@joedysart.com or visit his website at www.joedysart.com.