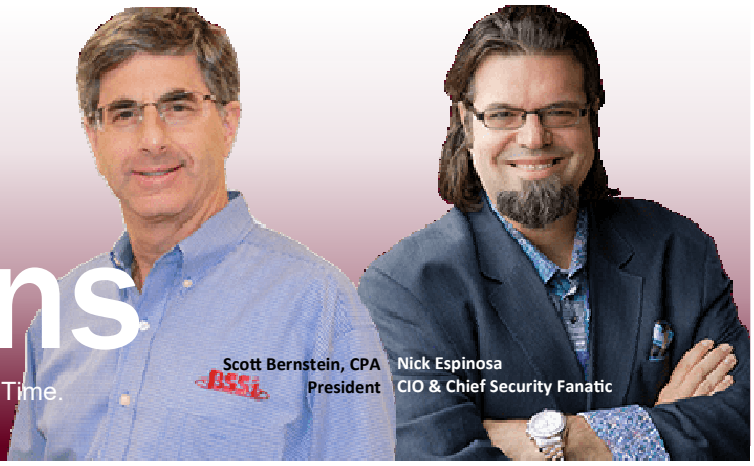
BSSi2

Innovations

Review Twice, Implement Once. Doing IT Right the First Time.



How To Make Sure You Never Fall Victim To Ransomware

Late last March, the infrastructure of Atlanta was brought to its knees. More than a third of 424 programs used nearly every day by city officials of all types, including everyone from police officers to trash collectors to water management employees, were knocked out of commission. What's worse, close to 30% of these programs were considered "mission critical," according to Atlanta's Information Management head, Daphne Rackley.

The culprit wasn't some horrific natural disaster or mechanical collapse; it was a small package of code called SAMSAM, a virus that managed to penetrate the networks of a $371 billion city economy and wreak havoc on its systems. After the malicious software wormed its way into the network, locking hundreds of city employees out of their computers, hackers demanded a $50,000 Bitcoin ransom to release their grip on the data. While officials remain quiet about the entry point of SAMSAM or their response to the ransom, within two weeks of the attack, total recovery costs already exceeded $2.6 million, and Rackley estimates they'll climb at least another $9.5 million over the coming year.

It's a disturbing cautionary tale not only for other city governments, but for organizations of all sizes with assets to protect. Atlanta wasn't the only entity to buckle under the siege of SAMSAM. According to a report from security software firm Sophos, SAMSAM has snatched almost $6 million since 2015, casting a wide net over more than 233 victims of all types. And, of course, SAMSAM is far from the only ransomware that can bring calamity to an organization.

If you're a business owner, these numbers should serve as a wake-up call. It's very simple: in 2018, lax, underfunded cyber security will not cut it. When hackers are ganging up on city governments like villains in an action movie, that's your cue to batten down the hatches and protect your livelihood.

The question is, how? When ransomware is so abundant and pernicious, what's the best way to keep it from swallowing your organization whole?

1. Back Up Your Stuff

If you've ever talked to anyone with even the slightest bit of IT knowledge, you've probably heard how vital it is that you regularly back up everything in your system, but it's true. If you don't have a real-time or file-sync backup strategy, one that will actually allow you to roll back everything in your network to before the infection happened, then once ransomware hits and encrypts your files, you're basically sunk. Preferably, you'll maintain several different copies of backup files in multiple locations, on different media that malware can't spread to from

Continued on page 3

Beware of a New Blackmail Phishing Scam

We've seen an influx of a new phishing scam going around - this scam utilizes data like email and passwords from various data breaches to blackmail you into sending money. Sometimes called a Sextortion Scam, the email message purports to have been sent from a hacker who's compromised your computer and used your webcam to record a video of you while you were watching porn. The missive threatens to release the video to all your contacts unless you pay a Bitcoin ransom.

Most often the hacker will spoof your email address (hiding the actual email address and making it look like came from yourself or someone else inside your organization) and/or include an example of your password for "proof" that they have hacked into your system. They then try to blackmail you into sending money so that they don't destroy your system or publish embarrassing information about you.

Understand that these are scams and no one has actually hacked into your system. **It is OK to delete and ignore these type of emails.** These are a type of blackmail and they are possible because of the many data breaches of different companies (for example, Target, Equifax, Yahoo!, and others). The information included in the email has been published and is available on the dark web for anyone to use.

This is a relatively easy way for scammers to extract money from you without have to have any real technical knowledge. **DO NOT pay any ransoms, reply to the scammers, follow any links, or open any attachments**. If the password included in the email is your current password **change your password ASAP**. Any place you use that password, change it. DO NOT USE the same password in more than one site. If one bad-guy has access to it then others do and may launch a more harmful attack with the information.

This type of email is just a trick, but it DOES highlight the importance of not reusing passwords. We hope this information helps. Please let us know if you have any questions or concerns regarding a scam like this.

**This article was originally posted in our weekly Security Tips email. If you'd like to be on that mailing list contact jhembd@bssi2.com*

From: [redacted]
Sent: Monday, October 1, 2018
Subject: account was hacked
To: [redacted]

Hello!
I'm a member of an international hacker group.

As you could probably have guessed, your account [redacted] was hacked, because I sent message you from it.

Now I have access to you accounts!
For example, your password for [redacted] is [redacted]

Within a period from July 7, 2018 to September 23, 2018, you were infected by the virus we've created, through an adult website you've visited.
So far, we have access to your messages, social media accounts, and messengers.
Moreover, we've gotten full damps of these data.

We are aware of your little and big secrets...yeah, you do have them. We saw and recorded your doings on porn websites. Your tastes are so weird, you know..

But the key thing is that sometimes we recorded you with your webcam, syncing the recordings with what you watched!
I think you are not interested show this video to your friends, relatives, and your intimate one...

Transfer $700 to our Bitcoin wallet: 13DAd45ARMJW6th1cBuY1FwB9beVSzW77R
If you don't know about Bitcoin please input in Google "buy BTC". It's really easy.

I guarantee that after that, we'll erase all your "data" :)

A timer will start once you read this message. You have 48 hours to pay the above-mentioned amount.

Your data will be erased once the money are transferred.
If they are not, all your messages and videos recorded will be automatically sent to all your contacts found on your devices at the moment of infection.

You should always think about your security.
We hope this case will teach you to keep secrets.
Take care of yourself.

Continued from page 1: How To Make Sure You Never Fall Victim To Ransomware

your primary network. Then, if it breaches your defenses, you can pinpoint the malware, delete it, then restore your network to a pre-virus state, drastically minimizing the damage and totally circumventing paying out a hefty ransom.

2. Get educated

We've written before that the biggest security flaw to your business isn't that free, outdated antivirus you've installed, but the hapless employees who sit down at their workstations each day. Ransomware can take on some extremely tricky forms to hoodwink its way into your network, but if your team can easily recognize social engineering strategies, shady clickbait links and the dangers of unvetted attachments, it will be much, much more difficult for ransomware to find a foothold. These are by far the most common ways that malware finds it way in.

3. Lock It Down

By whitelisting applications, keeping everything updated with the latest patches and restricting administrative privileges for most users, you can drastically reduce the risk and impact of ransomware. But it's difficult to do this without an entire team on the case day by day. That's where a managed services provider becomes essential, proactively managing your network to plug up any security holes long before hackers can sniff them out.

The bad news is that ransomware is everywhere. The good news is that with a few fairly simple steps, you can secure your business against the large majority of threats.

Technology Tidbit

Top Training Tips To Improve Your Team's Customer Satisfaction Skills

When customers leave dissatisfied after interactions with your business, the problem is likely more systemic than you realize. It can be hard to get a handle on poor customer satisfaction, but one of the best ways to address it is through comprehensive onboarding and training programs for your employees.

Don't make training a grueling info dump — the human mind can take in only so much data at once. It's best to split up your training programs into manageable chunks to ensure all the information gets absorbed. And give employees the tools to manage their own training. The ability to dip in and out of training modules allows them to move at their own pace, which greatly increases retention rates. Most importantly, don't waste your employees' time with big, clunky meetings, when individually tailored programs will suffice.

-SmallBiztrends.com, 7/20/2018

On The Lighter Side

Q: What do you use to mend a jack-o-lantern?
A: A pumpkin patch.

Q: What did the oak tree say when autumn came around?
A: Leaf me alone.

Q: How are you supposed to talk in the apple library?
A: With your incider voice.

Q: Why did the scarecrow win the Nobel Prize?
A: Because he was out-standing in his field.

Q: What did the doctor say when the nurse told him the invisible man was there?
A: Tell him I can't see him.

Q: What is the ratio of a pumpkin's circumference to its diameter?
A: Pumpkin Pi

Q: Why did Humpty Dumpty have a great fall?
A: To make up for his miserable summer.

Q: Why do trees hate tests?
A: Because they get stumped by the questions

October 2018

35 Aztec Court
South Barrington, IL 60010
(312) 752-4679
www.bssi2.com

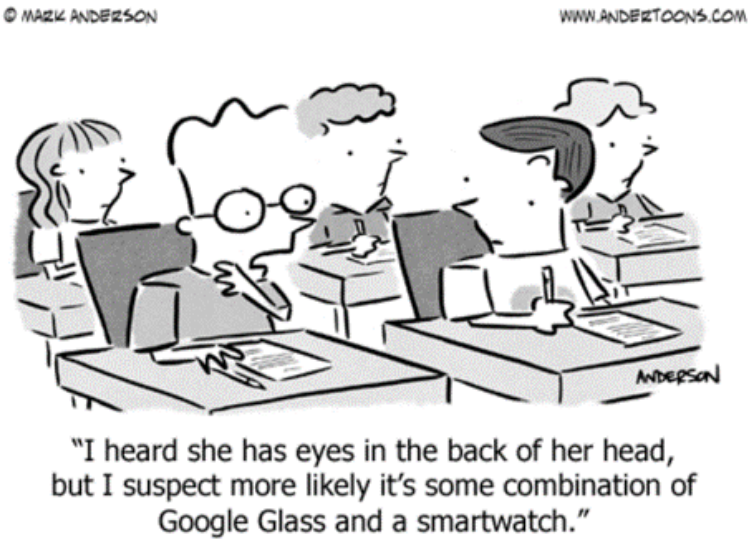
"We make all of your computer problems go away without the cost of a full-time I.T. staff"

Shiny New Gadget of the Month

Clocky
The Alarm Clock On Wheels

Waking up can be difficult. Even the most driven people occasionally struggle to get out of bed in the morning, pounding the snooze button ad infinitum until we finally force ourselves upright, dazed and groggy from interrupted sleep.

That's where Clocky, the alarm clock on wheels, comes in. Clocky is an adorable little digital timekeeper to keep by your bed; it will be your best friend until it comes time to rise in the morning. By default, it'll give you a single press of the snooze for free, but once you hit snooze for the second time, it'll speed off and start wheeling around your room, beeping and making a racket until you catch it and send it back to sleep. If you or someone you know struggles to get out of bed in the morning, Clocky will be a trusted ally in your mission to start the day.



"I heard she has eyes in the back of her head, but I suspect more likely it's some combination of Google Glass and a smartwatch."

Stay up-to-date with the latest Cybersecurity News!

Follow our Chief Security Fanatic and CIO, Nick Espinosa, on social media for cybersecurity videos and articles:

f www.facebook.com/NickAEsp

twitter.com/NickAEsp

in www.linkedin.com/in/nickespinosa/

Follow BSSi2 at:

f www.facebook.com/bssi2

twitter.com/BSSi2llc