Rochester Business Journal
FEBRUARY 15, 2019

SPECIALREPORT

Cybersecurity

‘THINGS’ CAN HURT

Beware of internet devices’ vulnerabilities

BY GINO FANELLI

Story begins on page 12

Internet of things in the vanguard but vulnerable to hacks

Experts eager to see standardization of devices to help ease safety concerns

By GINO FANELLI

You'd be hard-pressed to find an everyday appliance that doesn't have an internet-enabled version.

Interested in a Bluetooth-enabled toothbrush that tracks your oral hygiene? Beam from Suitable Technologies Inc. and Oral-B from Procter & Gamble Co. have options for that.

Need a wireless sound system built right into your office chair? There are seemingly an infinite number of options available for that.

How about a smart dog collar that not only keeps track of your dog's location, but also the number of steps taken and how hot or cold they are? Would you like that in leather or sport?

As inexplicable as many of these products may seem, there is no question among tech industry experts that the future lies in the "internet of things," or IoT, a method of creating products connected in some way to the internet. From advanced car tech to Amazon Echoes, IoT is quickly touching every facet of daily life and it's becoming bigger and bigger business. According to a study by Boston-based global consultant Bain and Co., the global IoT market is expected to hit $520 billion in 2021, more than double the 2017 number of $235 billion.

But experts in the world of cybersecurity see a need to pump the brakes a bit, noting that bad actors get more chances to breach people's or business's networks the more they integrate products with internet capability.

"I don't think we have any choice," said Paul Greene, a partner at law firm Harter Secrest & Emery LLP who leads the firm's privacy and data security practice. "We, as a society, love and hate surveillance, we want targeted advertisements, we want a better deal on things than our neighbors, we want devices that will open our car and lock our house doors, but, at a certain point, things shift and they seem creepy."

"Creepy," in Greene's sense, means the invasion of privacy that a good chunk of IoT tech fosters. Fears of an "always listening" device have existed since the explosion in popularity of the Amazon Echo or Google Home. While the companies deny that they spy on their users to create targeted advertisements, the tech is there. Looking past the valid fear that these devices could inadvertently record and transmit a private conversation, which happened to one Echo-owning couple last year, the larger concern revolves around just how secure these brainy tools really are.

Rochester's Innovative Solutions sees difficulty arising from how varied and unstandardized IoT devices are. They are more and more of them, with varying software, said Bill Knitter, director of IT services. "The challenges we have with traditional mobile device management are all exacerbated with managing IoT devices."

Echo, Google Home and Siri for iPhone all function based on an always-on microphone. The devices are always listening, recording short samples of ambient sound and deleting them until they are activated by their trigger phrase ("Alexa," "Okay Google" and "Hey Siri," respectively). Of course, these devices can all be hacked, although large tech companies have good incentive to create their own internal cybersecurity protocols to protect users.

"If you really are a Google person, you can have a Google account that controls all of the devices that you have in your home, in your car and on your phone, … and you can get a report every day from Google telling you what needs to be updated and what the risks are," Knitter said. "Just like when a credit card company calls you and tells you your credit card is at risk."

Knitter calls this a very company-powered, free-market capitalist solution to the security issue that can make IT consultants' lives easier. However, it's a solution that leads right back to the issue of standardization. If there is no sweeping protocol in place that says what sort of security measures are needed to protect users, each company's products will secure themselves differently. Some might have tight, easily monitored security measures. Others may be loose or easily compromised, and if one part of a user's network is broken, the entire system can be compromised.

There have been many, many data breaches through IoT, the majority of which didn't cause lasting damage. Some were deeply unsettling.

"Putting aside the issue of how IoT can help companies, I'm really focused on how they can harm them," Greene said. "Every IoT-connected device is a surface area that can be attacked on a network. It is a vehicle that can provide protected or otherwise sensitive information to a threat actor, and it's also a weapon that can be used against even unrelated networks in the form of denial of service attacks or IoT-launched attacks."

A denial of service attack is a form of cyberattack that causes massive numbers of fake requests to be sent to a specific server, causing difficulty for legitimate users to gain access. On Oct. 21, 2016, hackers were able to use a massive number of unprotected internet-enabled devices to launch a denial of service attack against domain name system Dyn, which in turn caused a large number of popular websites, including Reddit, Tumblr and Yelp, to be inaccessible. A total of three attacks were launched throughout the day.

That collection of devices is known as a "botnet," a series of unrelated and unprotected devices infected with a virus that, in tandem with hundreds or thousands of other devices, are used to launch attacks, steal data or send spam. It's nothing new—if your computer has ever had a virus it's likely it was used for a similar purpose.

IoT, however leaves more holes for the hackers to leak in.

"That's the new reality for entities large and small," Greene said. "It's a danger that many people are crying wolf about, but maybe it's not really wolf that they're crying. We've seen IoT denial of service attacks—that's been around for a number of years now—but until that starts to affect Main Street, the magnitude of that threat won't begin to be fully understood."

In context, there have been many, many data breaches through IoT, the majority of which didn't cause lasting damage. Some were deeply unsettling, such as the case of the man who hacked into a Houston couple's Nest baby monitor to hurl sexual expletives at their baby late last year. And in typical internet fashion, some were just racist, sexist, homophobic or anti-Semitic, such as the case of the "white supremacist hacktivist" who broke into unprotected printers across North America to print ads for a white supremacist website, complete with swastikas, in 2016.

Ultimately, Greene sees an inevitability that there will be a moment where real security protocol will become the norm in IoT devices, but to make that happen, it's likely going to take some sort of trouble. He compares it to the payment card industry data security standard (PCI DSS), an industry-wide information security standard for payment and credit cards, established in 2004.

"Unfortunately, it may take a problem," Greene said. "A lot of the legislation in this space is reactive rather than proactive. Even PCI DSS came about because of an explosion in credit card related breaches and the realization that security, in many cases related to payment cards, was abysmal."

gfanelli@bridgetowermedia.com/ (585) 653-4022

Data in danger of being snatched once it leaves the office

Encryption, vigilant employees best barriers to ever-present cybercrime

By MIKE COSTANZA

Be careful when you hit "send."

"Once that data leaves your network in your office, you lose all control of it," says Matthew Topper, chief technical officer for CAPSTONE Information Technologies Inc. "The only thing you control is what happens to it before it leaves."

Topper

Marcellus

Businesses that don't safeguard their data risk suffering breaches of company or customer files.

"This can cause reputational harm, loss of business, loss of trust, loss of intellectual property, and effect numbers of businesses and individuals," says Dan Marcellus, president, CEO and founder of SkyPort IT Inc.

Small and medium-sized businesses can be hit particularly hard.

"Security's always been a concern with IT (information technology), but probably in the last six years, the threats have become business-crippling," says Frederick Brumm, vice president, co-founder and co-owner of CE-Technologies.

Data becomes vulnerable at a number or points as its being transmitted over the Internet, beginning with the fiber-optic or copper lines over which it travels.

"It is possible to break into all of those… just like the old phone taps did," Topper explains.

As the data goes through, those tapping into the line can access it.

"It's not quite as straightforward as hooking up a phone line, but if the data's not encrypted, you can certainly glean useful information out of that if you're willing to sort through it," Topper says.

Cybercriminals can access data-in-transit by other means, as well. While traversing the web, files at some point will reside on an Internet service provider's servers. An ISP usually rents spaces on one server to multiple customers.

A barrier called a "hypervisor" walls off the data and programs on one part of the ISP's server from those on another part. None of the businesses on the device can detect each other, so each one appears to have its own server. Breaches of hypervisors are extremely rare, but serious.

"Breaking into that allows access to all of the servers running on top of it. That is the crown jewel," Topper says.

Data can be vulnerable to other threats, as well.

"End users are the biggest threat," Brumm asserts "Employees that don't know what websites they should not go to, what downloads they should not install on their computers."

Phishing, is a social engineering technique, in which a website or individual fraudulently impersonates one that is legitimate. A website might have a "Microsot.com" address instead of Microsoft.com." Someone who didn't notice the difference might send important information—a username, password or even his or her company's data—to the site.

"You get phishing emails saying 'Send it here.' All of a sudden, you've sent it to the wrong people," Marcellus explains.

Sometimes, the "phishing expedition" involves infiltrating a business or nonprofit. A criminal might first email, then call, and then visit the appropriate person at a firm, all to gain a way into its files.

"It's all about building up the trust over time," Marcellus says.

The wrong click of a mouse can also download a deadly CryptoLocker virus to company computers. The program, a form of ransomware, then encrypts the firm's data files.

"Now that the data is encrypted, the criminal then demands ransom, and that ransom is typically paid in bitcoin," Brumm explains.

Though it's sometimes possible to decrypt a company's data files, the process can be so difficult, time consuming and expensive that the firm chooses to pay the ransom.

Companies can take a number of steps to prevent criminals from accessing their files. To begin with, data should be encrypted before being transmitted. When run through an encryption program, files come out as unintelligible glop that cannot be interpreted without the proper key.

There are two basic forms of high-level encryption: symmetric and asymmetric. In symmetric encryption, the sender and receiver of the data use the same key. That presents a bit of a problem.

"I need to have some way to exchange that key, a supposedly secure communication channel," Topper explains.

In asymmetric encryption, the sender uses one key to render the data unintelligible, and the receiver a second key to turn it back into a usable form. Though asymmetric encryption is more secure than symmetric encryption, symmetric can encode data at least 10 times faster. Some businesses use a combination of the two.

Continued on page 14

Best defense against cyberattacks are well-trained employees

‘I can’t stress how important it is to build that human firewall’

By **SETH WALLACE**

Protecting your information gets harder every day, whether you know it or not.

It’s never been easier for bad actors to acquire and wield sophisticated tech tools to target your business, your financials or your privacy. As anyone who’s tried to keep up knows, it’s a full-time job — often many full-time jobs requiring a dedicated department and budget.

The face of cybersecurity has changed in drastic ways, unrecognizably and almost beyond hyperbole, since companies first started installing dial-up connections in the 1980s. You’re undoubtedly familiar, however, with the faces that will feel the effects of your cybersecurity policies — they’re the employees that show up for work every day.

“I can’t stress how important it is to build that human firewall,” said James Keeler, a cybersecurity expert with Rochester’s LMT Technology Solutions. “The real magic, the sweet spot, is when you sit down and assess what you need to protect and how to do that while still allowing your company business to flow.”

Keeping out the bad guys while letting in the good guys is a problem that has vexed tacticians since the first humans put pointy sticks outside the cave. Sharp end goes that way (sabertooth tiger, dangerous), but what if my friend wants to come in? Some concepts are timeless, but we’ve come a long way.

“From a top-down perspective, you have to very carefully balance your security and convenience plans,” said Keeler. “Security comes at a cost and that’s usually convenience. Every little step to stop attackers makes it harder for your employees to get a process completed.”

According to Dan Marcellus of managed security service provider SkyPort IT, most companies would benefit from taking a hard look at their baseline, ground-level policies and procedures, regardless of their field.

“Your typical employee handbook does not hack it, pun intended,” Marcellus said. “There’s a big gap between the marriage of security and policy.”

For those of a certain generation who still remember when computer security revolved around 3.5-inch floppy disks passed around the office, it can be almost dizzying to look at how far the IT business has come.

“As late as 2007, the biggest threat was jamming up your email, maybe crashing a server or letting in a lot of spam,” said Keeler. “In the last five years, the damage and extent of the threats facing companies is coming to light and now you’re worried about if they’re stealing the core of our business and manufacturing it in China.”

For a prime example of the havoc a security breach can reach, Rochesterians don’t have to dig back far in the memory bank to remember 2015, when local health care management provider Excellus reported a breach of millions of patients’ information.

“There’s no more saying, ‘oh well, the IT guys can just fix it,” said Keeler. “One incident can put you out of business.”

Keeler said in the case of Excellus, the exceedingly expensive data breach would’ve easily put a small company out of business.

Whether starting from scratch or adapting policies and procedures to your existing business, security experts agree on one thing: he or she who hesitates is lost.

“Hackers are smart and if we’re asking businesses to take advance of big data and artificial intelligence — all this great new technology — the hackers are taking advantage as well,” said Michael Montagliano, security impresario at Rochester’s iV4.

Montagliano said in 1988, the National Vulnerability Database, the U.S. government repository of standards-based vulnerability management data, showed two national security vulnerabilities. That number is now more than 16,000. In the early 2000s, almost 300 new pieces of malware (harmful software) were released every day. Now? More than 300,000.

With modern society’s reliance on our devices and perma-connectedness, cybersecurity providers have to grapple with user habits, tendencies and sometimes, naiveties.

“We’re not telling our employees not to use Gmail because we want to be mean,” said Keeler. “We know there’s X number of infections coming through this vector and that infection could take down the company.”

If a company supplies to the Department of Defense on a contract, congressional regulations and DFARS (The Defense Federal Acquisition Regulation Supplement) mandates protection of “confidential unclassified information.”

“That’s a response to foreign actors, China, Russia, stealing our intellectual property,” Montagliano said. “If they’re hacking our Department of Defense supply chains and stealing blueprints for missile technology or putting in a fraudulent switch that looks like Cisco — that’s a backdoor into China.”

“Regulations and milestones” go up and downstream from producers and supplies to end users, showing even the highest levels of government are training an eye on the problem.

The orders of magnitude are stark and the challenge for businesses is clear: harden your security and educate your people. All levels of your organization need to be keenly aware of both the threats extant and countermeasures in place to protect your security integrity, including subcontractors and vendors.

“Training your employees is critical because they’re the easiest way to breach a company,” Montagliano said. “User error can circumvent all layers of protection with one click if you have someone blindly trusting someone is who they say they are.”

E-mail-based scam and fraud is still the top culprit of business data intrusion. Federal law enforcement estimates more than half of all business data breaches are due to fishing campaigns, and there’s a direct correlation between the amount of time companies put in to training their employees and the strength of your defense.

In a baseline fishing (emails designed to illicit a click) campaign, Montagliano said, typically 19 to 21 percent of users will succumb. After six months of training, that drops to 12 percent. After a year, it’s down to 2 percent. Ongoing security reminders, remedial training and “nudging the culture” are part of the entire “critical security training loop.”

Montagliano said he recently attended a cybersecurity symposium featuring representatives from the FBI.

“They said, ‘if I was going to allocate my entire budget, it would be to training my people.’”

Seth Wallace is a Rochester-area freelance writer.

DATA

Continued from page 13

“Using the combination allows you to have the benefits of symmetric encryption with the security benefits of asymmetric encryption,” Topper says.

Encryption might also be used to safeguard information that’s not headed to the web—say, credit card data, personnel files and the like.

“Say you’re transferring data from one internal server to another—it could be sensitive data,” Marcellus says. “If you’re not doing that in an encrypted sense in your internal network, it is possible for someone in that network to monitor and see that data.”

Most computer programmers and IT vendors do not write their own encryption programs. Instead, they turn to software firms—Microsoft’s operating system, for example, has encryption built in. A lot of CAPSTONE’s customers use Microsoft Office 365.

“Office 365 has a mechanism to send encrypted, secure emails natively,” Topper explains. “We’ll help customers determine if that is appropriate for them, and if so, set that up, and go through how to use it, how to monitor it.”

Even when such measures are in place, human error can render them useless.

“We find business owners sending passwords and credit card information and personally identifiable information through email,” Brumm says. “If somebody picks up on the right piece of information, they could go out of business.”

To minimize the risks of such errors, firms need to establish strict procedures for the safe handling and transmission of data, and train their employees to use them. CE-Technologies offers an online course on the dangers of the net.

“At the end of the day, they know what to look out for on the Internet, what emails are legit, what emails are not legit,” Brumm explains. “They know how to decipher what’s a phishing email, what’s not a phishing email. They know what CryptoLocker viruses are, and what to do with them.”

Most of SkyPort’s business comes from medical offices. The firm will go so far as to use social engineering techniques to test customers’ data security systems.

“We’ve gone in, and we’ve got people handing us admin passwords. It’s just incredible what people will do to try to be nice,” Marcellus explains.

Perhaps the best way for companies to safeguard their sensitive data is to not send it out over the net at all.

“Our biggest advice is to not transmit sensitive information if there’s not a legitimate business need to do so,” Topper explains. “There’s always a risk.”

Mike Costanza is a Rochester-area freelance writer.