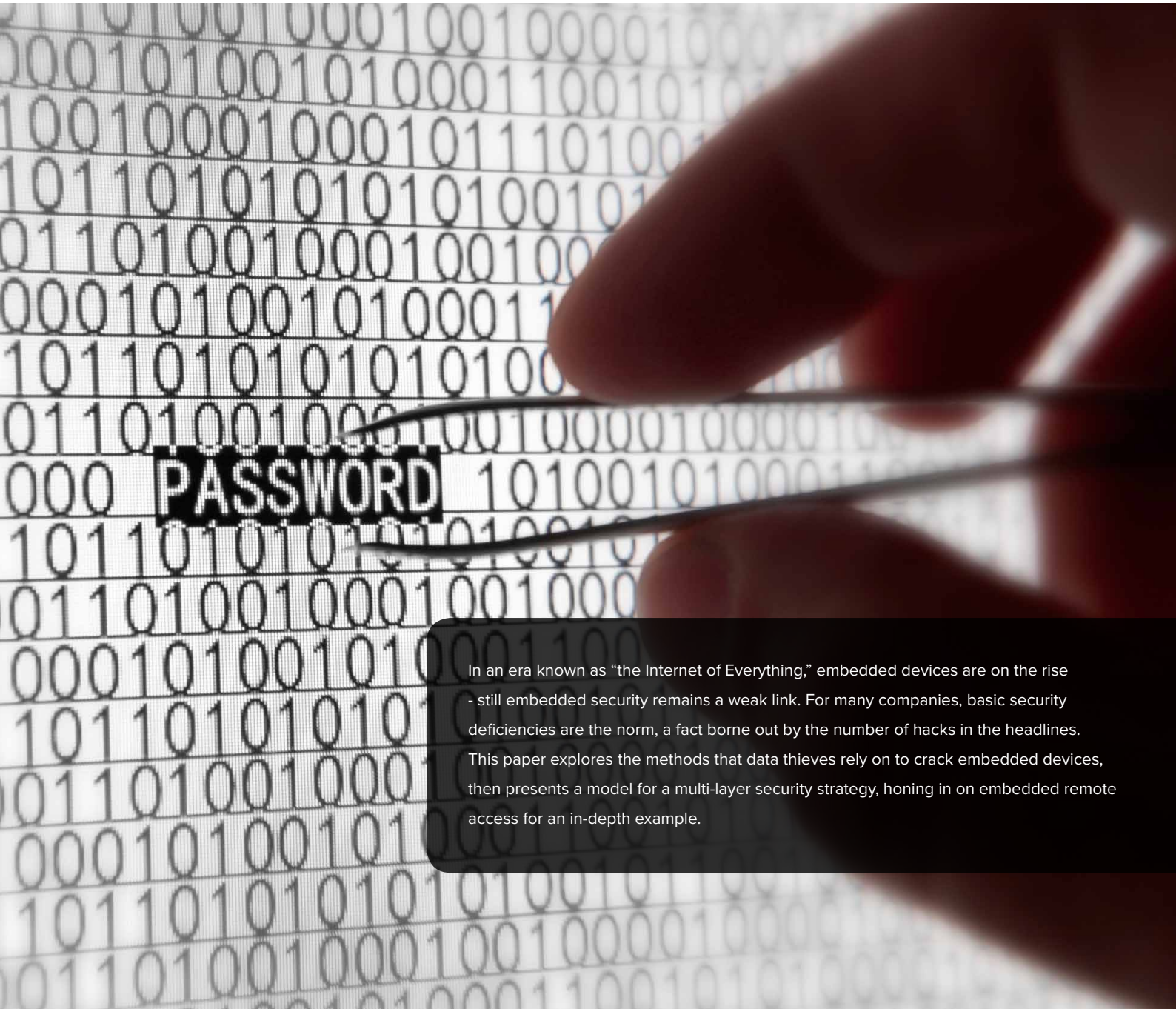
SECURITY PAPER

NETOP Remote Control

Embedded Devices & Data Thieves: Understanding the Vulnerabilities



In an era known as “the Internet of Everything,” embedded devices are on the rise - still embedded security remains a weak link. For many companies, basic security deficiencies are the norm, a fact borne out by the number of hacks in the headlines. This paper explores the methods that data thieves rely on to crack embedded devices, then presents a model for a multi-layer security strategy, honing in on embedded remote access for an in-depth example.

The Internet of Everything

It's called the Internet of Everything—a fast-paced, wide-sweeping movement in the IT industry to connect it all: to take an overwhelming variety of objects, devices, processes, both physical and digital, and get them talking to each other.

Devices, Devices Everywhere

The people driving this movement paint some vivid pictures. Imagine you're caught in a natural disaster—and rescued, because your sneakers told first responders where you were. Imagine "sensors on cars talking to data centers that talk to cell phones that talk to blood pressure monitors" (Forbes, 2013). Or, as you're walking out of the office for the day, imagine telling your iPad to turn on the porch light at home, queue up some music and bump the thermostat a few degrees higher.

It's not an episode of the Jetsons. It's happening. As multinational tech company Ericsson put it, "This marks the beginning of a new era of innovative, intertwined, combined products and services that utilizes the power of networks" (2011). In fact, Ericsson predicts that by 2020, the number of connected devices will grow to 50 billion.

As the IoE movement continues to develop, embedded devices stand to become ever more ubiquitous. The question is, will security keep up?

The significance of this is, in a word, big:

Several big companies have identified it as a giant opportunity—Amazon, Cisco, Ericsson, GE, IBM and Qualcomm among them. They all believe that what many call the Internet of Everything (or IoE) could have an even bigger impact on the world than the Internet that preceded it. (FORBES, 2013)

From a security standpoint, this is both both good and bad.

The Crime of the Future

Not that long ago, cyber security used to seem like a big dark cloud that no one knew much about—the stuff of which spy movies are made. Yet since the first motions toward IoE, headlines have been bristling with hacker stories.

In 2012, our connected world of machines, devices, people and networks resulted in more than 900 reports of theft or loss of data with six instances resulting in nearly 40 million records being compromised. Despite numerous warnings, extensive media coverage and corporate security policies, companies continue to struggle with cyber threats. (FORBES, 2013)

Given the sheer number of connections that exist (and with innovative new connections continually emerging), it's fair to state that these days, no company can afford to remain casual about security. Everyone is a target: retail, finance, leisure, travel, businesses large or small, from enterprise organizations all the way down to the local brick-and-mortar.

Embedded Devices - a Special Kind of Vulnerable

CSO Online called embedded devices "eons behind" where security is concerned: "One of the biggest challenges in security today is how the software in our operating systems and applications are so full of holes" ("Embedded system security," 2012).

Furthermore, these devices are ubiquitous. Almost every business relies on embedded technology to some extent: point-of-sale devices, ATM machines, kiosks. As the IoE movement continues to develop, embedded devices stand to become ever more ubiquitous. The question is, will security keep up?

It will have to. POS attacks are "growing exponentially," according to Tom Kellerman, the VP at security company Trend Micro ("Hacker News," 2012)—to say nothing of attacks on other types of embedded devices—and they're not affordable.

In the following section, we'll delve deep into the world of data theft, specifically as it pertains to embedded devices—how data thieves achieve access, how much a breach costs, who's vulnerable and what you can do to protect your organization.

Embedded Devices & Data Thieves

Know Thy Enemy

A hacker's goal is simple; they're looking for data they can turn into cash. Hackers themselves, however, appear to be somewhat more complex. According to Verizon's 2012 Annual Data Breach Investigations Report, most data thieves are professional criminals.

For example, take the four Romanian hackers who, between 2009 to 2011, cracked the POS devices of over 150 Subway franchises. Their conspiracy was enacted on a such a scale, Ars Technica said, it compromised 146,000 cards, cashed in $3 million in fraudulent charges and inflicted $10 million in losses ("How hackers gave Subway a $3 million lesson," 2011).

If you prefer books to sandwiches, consider the 2012 Barnes & Noble breach. Credit card data was stolen from 63 stores in a multi-tiered attack; here again POS devices were the inroad. "This is no small undertaking," said RSA's chief security officer Edward Schwartz. "An attack of this type involves many different phases of reconnaissance and multiple levels of exploitation" (New York Times, 2012).

This style of data theft has evolved from exotic to common. "It's the crime of the future," said Dave Marcus, McAfee Labs director of security research and communications, speaking to Ars Technica about the Subway breach.

So while the goal itself may be simple, bear in mind that today's professional data thieves are sophisticated enough to tread where a previous generation might not have gone—such that now, even "a national retailer with stores in almost every major city across the United States" isn't too daunting a target ("Hacker News," 2012).

IT WON'T HAPPEN TO ME

For every company that suffers a compromise, there are many that do not. Verizon even has an acronym (WIBeHI: "wouldn't it be horrible if") for the kind of breach scenario that can replay ad nauseam in a sleepless executive's mind; happily, for many, these fears don't come home to roost (2012).

On the other hand, when one is dealing with the consequences of a data breach, it's no comfort to consider how improbable you thought it was. "We know at least four victims that are no longer in business, either wholly or in large part because of their breach," Verizon said. The risks are real.

Here Come the Consequences

What does a company stand to lose? When a hacker cracks your embedded devices, payment card data is often the first casualty and the proportions can be rather epic. Hacker Factor, a computer forensics research organization, speculated that major retailers such as Target are likely to be storing over 58 million cards on their branch server at any given time, and stored data is potentially stolen data (Hacker Factor, 2007).

As it turns out, 58 million is not a bad guess. In 2011, Sony Corporation suffered a breach that impacted 77 million records; in 2012, Zappos saw 24 million impacted. Heartland Payment Systems topped the list, with 130 million records impacted in 2009.

Of course data isn't the only thing to lose; there's also money. When TJX Companies saw 94 million records compromised in 2007, it translated to over $64 million in damages. Following on the heels of a breach are legal costs. Then there are the intangibles: branding, reputation, public relations.

If your organization loses credit card or personal data, you incur notification, incident response, investigation and legal costs, along with a PR nightmare, potential customer churn and possible fines and lawsuits.
(THE POINT-OF-SALE PROBLEM, 2009)

Altogether, the total costs of a data breach are hard to calculate. Businesses often don't report on it, Verizon said; also, downstream impacts complicate the equation: "the impact is often felt by organizations that are not the breach victim… These downstream effects are often neglected when considering the overall consequences of data breaches" (2012).

YOUR DATA, UNDER SIEGE

"Any system that's part of a payment process is a target of data thieves. Wise companies will assume that the devices, applications and networks that house sensitive cardholder data are under siege and act accordingly" (The point-of-sale problem," 2009).

Who's the Biggest Target?

In Verizon's 2012 dataset, the biggest victim among industries was retail, accounting for almost 22% of all network intrusions. Finance came in sixth at 8%. Transportation and accommodation accounted for 6.7% (2013).

Where devices are concerned, servers (including POS controllers) were an attractive source of booty for data thieves, as they store and process "gobs (technical term) of data" (Verizon, 2012). User devices (including ATMs, kiosks and POS terminals) may be even more vulnerable. Like servers, they store and process data; they're also widely distributed, less restricted and highly mobile. They also outnumber servers. They're also controlled by end users.

Perhaps this is why—of the compromised assets that Verizon investigated—user devices took the lead, accounting for 71% of the total. When one considers that in 2008 (a mere five years ago), these devices accounted for only 17% (Verizon, 2013), that's a high percentage indeed.

POS Devices

POS devices can easily become a hacker's treasure trove. Not only are they "one of the most frequently used computing systems in the developed world" ("The point-of-sale problem," 2009), the data they collect is comprehensive, including the card number, expiration date and full magnetic strip, "which makes it possible, for example, to encode that information on a dummy card for use at an ATM machine or a retailer" ("Cybercriminals," 2011).

Also, they're not hard to exploit:

There are many vulnerabilities within a POS system – if a system is not properly protected, anyone with an inside knowledge of how the systems work can carry out a hack without much difficulty. (CYBERCRIMINALS, 2011)

Hackers go where the getting is good. If one target resists their efforts, they tend to move on to other, easier targets.

Most of the data breaches studied by Trustwave—a company specializing in data security and PCI compliance—boiled down to weaknesses in POS devices ("Cybercriminals," 2011), which "continue to be the easiest method for criminals to obtain the data necessary to commit payment card fraud" (Trustwave, 2011).

ATM Machines

If POS devices present the easiest inroad, ATMs are possibly the most lucrative. Trustwave did not see as many compromised ATMs as POS devices, yet "while less frequent, when they are successful, they yield a payout many times larger than any other type of cardholder data breach" (Trustwave, 2013).

"Less frequent" is a relative term, by the way. Verizon found that ATMs represented 30% of compromised assets across the board in 2012.

As for their vulnerability, consider the Jackpot demonstration at the 2010 Black Hat security conference in Las Vegas ("Researcher demonstrates," 2010). Barnaby Jack—director of security research at IOActive Labs—demonstrated two ways, both local and remote, to crack an ATM within minutes onstage. Fifty-dollar bills came flying, but the deliverable can be just about anything the thief prefers—card numbers, pin numbers, cash—and a "fully loaded bank ATM can hold up to $600,000" ("Researcher demonstrates," 2010).

Jack's performance was staged, but the tactics he demonstrated are real enough. In 2009, ATMs throughout Russia and Ukraine were effectively breached using the same approach ("New ATM malware," 2009).

Kiosks

Kiosks deserve a place, too, on this list of vulnerable devices. For example, consider the 2012 breach in New Zealand, where the Ministry for Social Development (MSD) detected a security flaw on its public kiosks that made it possible to open sensitive files across the organization—including financial records, confidential client information, medical invoices, staff salaries and so on ("Why the MSD security breach matters," 2012). Like ATMs, kiosks are user devices running standard operating systems, which can be exploited either physically or remotely.

What To Do?

Don't Be the Weak Link

As we've been emphasizing, there is no such thing as safe territory for embedded devices in today's IT landscape. Still, there is a moral here. Hackers go where the getting is good. If one target resists their efforts, they tend to move on to other, easier targets.

On one hand, this makes the game more difficult: organized criminal groups are somewhat unpredictable. Instead of limiting themselves to big players with a lot to lose, they're happy to "pilfer smaller hauls of data from a multitude of smaller organizations" in a "high-volume, low-yield business model." They don't necessarily "follow the logical lines of who has money and/or valuable information" (Verizon, 2012).

Simply by putting good defenses in place, you can lower the odds that an attacker will invest any effort on you in the first place.

Target selection is based more on opportunity than on choice. Most victims fall prey because they were found to possess an (often easily) exploitable weakness rather than because they were pre-identified for attack. (VERIZON, 2012)

On the other, this is good news in disguise. Most attacks are opportunistic; this means that when companies adopt a multi-layer, defense-in-depth security strategy, to some extent they can prevent data thieves from even trying.

These Attacks were Not Rocket Science

The very simplicity of the attacks we've been discussing bears this out. "Onerous" is not a word one would use to describe them. Ninety-six percent of the breaches that Verizon investigated in 2011—"the great majority," targeted or not—were not highly difficult (2012). In most cases, hackers relied on rudimentary methods, automated tools and scripts, no customization and modest resources (Verizon, 2013).

To an alert reader, this may come as a surprise. Earlier we pointed out that our current generation of hackers is more sophisticated than those that came before—so why are they using such elementary methods? Why not flex their technological muscles?

To be blunt, they don't have to. The low difficulty of data breaches over the last two years reflects less on the hackers than it does on the victims, whose skill and readiness just didn't require much to overcome. Herein lies the good news. A lack of skill and readiness can be remedied.

Creating Your Security Strategy

A Few Considerations

Data breaches are a multi-faceted problem, and a "one size fits all" approach will not do (Verizon, 2013). Rather, your security strategy should grow out of your particular threat landscape. Below are a few general considerations to bear in mind.

First, make your strategy a priority. When the MSD kiosk security failure hit the news in New Zealand, it detonated a scandal—not due to the consequences of the breach (which was discovered by IT workers, not data thieves), nor only to the gravity of the potential fallout (whose victims would have included a vulnerable group of at-risk youth). Rather,

Labour and Green party spokespeople railed against the government for the negligence that made the flaw possible in the first place, given "just how simple it would have been to create a secure network or fix the security issues when they first became apparent" ("Why the MSD security breach matters," 2012).

Likewise, in the Subway scenario: "these people weren't thinking about point-of-sale-security—they were just thinking about making a sandwich" ("How hackers gave Subway a $3 million lesson," 2011). Both organizations, for various reasons, allowed security to slip from the picture. It happens. Be sure not to let it happen to you.

Second, comply with regulatory standards (e.g., PCI) and follow manufacturer security guidelines (e.g., changing default passwords). According to Trustwave, "these controls are rarely implemented properly" ("Cybercriminals," 2011). In fact, Verizon reported that 96% of its 2012 breach victims—an astonishing majority—were not PCI-compliant at their last assessment, or had never been assessed in the first place (2013). "Nearly every case that we have seen thus far has attributes of its breach that could have been prevented if the control requirements had been properly implemented," Verizon said.

Third, after you've done the above, don't consider the job complete. "We cannot stress enough," Verizon said, "that while compliance definitely helps drive security, compliance does not equal security" (2012). And while it's prudent to follow security recommendations from your POS, ATM or kiosk manufacturer, know that your vendor may "take a reactive approach to security"—a pattern Hacker Factor observed of POS vendors in particular, who generally don't initiate new security measures until a credit card provider requires it (Hacker Factor, 2007). Their guidelines are useful, certainly, but not comprehensive.

In short, assume an active posture. Evaluate your organization's vulnerabilities and develop a thoughtful, defense-in-depth security strategy with multiple layers of protection to deter data thieves at large, and interrupt those who do attempt to compromise your system. In our final section, we illustrate what a strategy of that caliber looks like.

HOW DOES YOUR ORGANIZATION COMPARE?

Verizon found that in 2011, 86% of large organizations were encrypting transmission of cardholder data and sensitive information across public networks. However, only 29% were restricting access to data by business need-to-know. Only 20% were assigning each user a unique ID, and only 11% were tracking and monitoring access to network resources and cardholder data.

Remote Access Security For Embedded Devices

A Closer Look at "Defense in Depth"

A good security strategy will involve numerous components, whose complete review is of course beyond the scope of this paper. In this final section, therefore, we'll focus on one important facet of your overall strategy: remote access security.

Why remote access? This type of software is a flexible, potent tool. If compromised, it can roll out the red carpet to data thieves, granting them hefty leverage inside a company's doors. It's also one of the most common tools to exploit. In Verizon's 2011 dataset, remote access software accounted for 88% of all hacking breaches, "more than any other vector" (2012).

Given the level of access that a strong remote control solution is designed to provide, and given how often this type of software ends up paving the inroad for data thieves, it would be difficult to overstate the importance of security when using a remote access solution to support your embedded devices.

Choose Your Solution Carefully

That is, choose a remote control solution equipped with the features you need to create a strong security strategy, from a provider with a history of IT experience and a demonstrated commitment to staying current in today's evolving IT landscape.

Especially for embedded devices, be sure its features meet your needs. Your remote access solution must provide the tools to deter sophisticated hackers, while also running within the stripped-down parameters of the devices themselves—a unique challenge.

Embedded systems traditionally have had very limited security options. Indeed, fitting a robust set of security features into such a small mechanical footprint can be challenging. (OVERCOME SECURITY ISSUES, 2007)

Of course, the solution must also be able to comply with mandatory regulations. "Whichever company you choose, most importantly, make certain that they are PCI-compliant" ("Three risks," 2013). Below is a short list of features to select for.

TEAM SPY: REMOTE ACCESS HACKING

Ten or so years ago, a group of attackers dubbed "TeamSpy" took a popular remote access program, hijacked it with malicious code and used it to spy on governments, companies and human rights activists throughout Eastern Europe and the Commonwealth of Independent States. Their activities weren't detected until 2012—almost a decade later (Kaspersky, 2013).

Industry-Standard Encryption

Perhaps the most obvious security defense when accessing embedded devices remotely is to encrypt your data. Choose a provider with industry-standard AES encryption or better.

Multi-Factor Authentication, Unique ID For Each User

Stolen credentials accounted for 76% of the investigations Verizon studied last year, "about four of every five breaches involving hacking in our 2012 dataset." This may be the "easiest and least-detectable way to gain unauthorized access" (2013).

If data thieves can guess, crack or reuse credentials that belong to someone else, they can leverage the access that goes with them. As tactics go, stolen credentials are fast, effective and easy. "It just doesn't take that long to pop a POS system using a scripted list of known usernames and passwords," Verizon said (2013).

To prevent this type of breach, Hacker Factor advises companies to assign a unique ID to each person with computer access (2007).

It also urges companies to stop using vendor-supplied passwords—which, surprisingly, many companies continue to do. After changing these passwords, create a schedule for updating them. Really this should go without saying, yet these "basic security deficiencies" are quite common, from the use of default passwords to single-factor authentication ("Cybercriminals," 2011).

Which brings us to our next point: choose a remote software provider with multi-factor authentication. Verizon said that if we could have replaced every single-factor password in the stolen credentials breaches of 2012, "it would've forced about 80% of these attacks to adapt or die" (2013).

Establish Remote Access Without Creating Backdoors

Alongside stolen credentials, backdoors top the list of popular hacker tactics—the same method that compromised Subway. According to Gary Taylor, executive director of the

Petroleum Convenience Alliance for Technology Standards (PCATS), the data thieves in that instance were "using bots to scan the web, looking for door knobs to jiggle" ("Breach exposes POS vulnerabilities," 2012). Ultimately, it was remote access software that created the backdoor.

According to the indictment, the systems attacked were discovered through a targeted port scan of blocks of IP addresses to detect systems with a specific type of remote desktop access software running on them. The software provided a ready-made backdoor for the hackers to gain entry to the POS systems. (HOW HACKERS GAVE SUBWAY A $3 MILLION LESSON, 2011)

Find out if your preferred remote access solution can establish access across firewalls without inadvertently compromising perimeter security defenses or creating backdoors.

Granular Privileges, Need-To-Know Access

Not all data thieves come from the outside. Some breaches start closer to home, with the abuse or misuse of privileges. This is an especial concern to enterprise organizations, where the abuse of privileges is most common.

To prevent internal misuse, Hacker Factor recommends restricting access to data "by business need-to-know" (2007). Verizon, too, includes the controlled use of administration privileges on its list of critical security controls (2013).

Your remote access solution should let you define granular user privileges and need-to-know security roles for every last technician, vendor and employee in your system. It should also give you centralized management over access rights, so you can decide—case-by-case or group-by-group—who is able to do (or view) what. When users exit your system permanently, you must be able to disable their permissions and confirm that their privileges have expired.

Extensive Logging, Monitoring

As we've emphasized, with a good security strategy in place, your organization is likely to deflect the attention of all but the most determined hackers. For those tenacious enough to attempt a breach anyway, your defenses should deter them. Still it's important to understand that no strategy is invincible.

If your organization were breached, how quickly would you notice? According to Verizon, most breaches go months or more before being detected (2013).

Defining a plan for detection and response isn't ancillary to a strong strategy; it has to be tied into the core of it. Hacker Factor urges companies to track and monitor all access to networks and payment card data (2007). Verizon's list of critical security controls includes the same advice (2013).

Choose a solution that lets you record each remote session and keep extensive records of what took place—down to the technician's mouse movements if necessary. You should be able to find out who established access, from where, to which device, when. If unauthorized changes were made, you should be able to see them. If a data transfer took place, your software should help you determine what was transferred, who transferred it, and where it was transferred to.

"Workers account for the vast majority of thefts in a retail environment... Point-of sale security weaknesses are simply new tools for them to use toward that end."

- BOLT INSURANCE AGENCY

Defining a plan for detection and response isn't ancillary to a strong strategy; it has to be tied into the core of it.

"We've come to the realization that many of the organizations covered in this report are probably not getting the message about their security."

- VERIZON RISK TEAM

Having these features in place, be sure to use them:

In 8% of breaches affecting large organizations, it was basic log-review and analysis that topped the internal active discovery list...this is one of the methods that we tout yearly, and believe to be more effective than nearly all other methods. How do we know this? Well, when we conduct an investigation, that's how we find the breach - reading the logs.
(VERIZON, 2012)

Remember, prevention isn't everything. In the event that you do face litigation or an audit, having a solid discovery-response process already in place will mitigate the time, costs and risks involved.

Centralized Management

As your organization grows and your infrastructure scales to accommodate it, complexity compounds, gaps proliferate and things can fall through them. So, choose a remote solution with a centralized console, from which you can support, service and maintain all of your devices. By doing so, you can harness the many divergent aspects of your embedded infrastructure into one manageable organism, improving security, workflow efficiency and peace of mind as well.

Conclusion

Security matters—yet with embedded devices, it's often neglected, often to a startling extent. When companies build their infrastructure on fundamental security deficiencies, they put an already vulnerable technology in harm's way, opening the door to exploitation.

Happily, alternatives exist. With intentional effort, an organization can create a multi-tiered strategy that deflects most hackers' attention in the first place, and can deter a focused attempt at compromise as well.

Whether you're setting up a new embedded infrastructure for your organization, or evaluating an existing infrastructure to ensure it's demonstrating best practices, we hope this paper provides the framework to help your organization avoid those pitfalls, and stand apart.

References

Bolt Insurance Agency. Four ways to strengthen your point-of-sale security. Retrieved June 24, 2013 from boltinsurance.com.

Breach exposes POS vulnerabilities: Hackers sentenced; court docs reveal attack details. (2012, September 19). Bank Info Security. Retrieved June 24, 2013, from bankinfosecurity.com.

Credit card data breach at Barnes & Noble stores. (2012, October 23). New York Times. Retrieved June 24, 2013, from nytimes.com.

Cybercriminals targeting point-of-sale devices. (2011, March 3). Computer World. Retrieved June 24, 2013 from computerworld.com.

Embedded system security much more dangerous, costly than traditional software vulnerabilities. (2012, April 16). CSO Online. Retrieved June 24, 2013 from csoonline.com.

Ericsson. (2011, February). More than 50 billion connected devices.

Everything changes with the Internet of everything. (2013, May 9). Forbes. Retrieved June 24, 2013, from www.forbes.com.

Hacker Factor. (2006-2007). Point-of-sale vulnerabilities. Dr. Neal Krawetz.

Hacker news: inside the Barnes & Noble data breach. (2012, October 25). iCorps Technologies. Retrieved June 24, 2013, from blog.icorps.com.

How hackers gave Subway a $3 million lesson in point-of-sale security. (2011, December 1). Ars Technica. Retrieved June 24, 2013, from arstechnica.com.

Kaspersky Labs. (2013, March 20). The 'TeamSpy' story—Abusing TeamViewer in cyberespionage campaigns: Version 1.02. Kaspersky Lab Global Research and Analysis Team (GReAT).

Netop. (2013). Remote access security: How big an issue is it? What can you do?

New ATM malware captures PINs and cash—updated. (2009, June 4). Wired. Retrieved June 24, 2013, from wired.com.

New trend: The point-of-sale system hack. (2013, April 16). iCorps Technologies. Retrieved June 24, 2013, from blog.icorps.com.

Overcome security issues in embedded systems. (2007, June 12). Embedded. Retrieved June 24, 2013, from embedded.com.

Researcher demonstrates ATM 'jackpotting' at Black Hat conference. (2010, July 28). Wired. Retrieved June 24, 2013, from wired.com.

The point-of-sale problem. (2009, December 5). Information Week. Retrieved June 24, 2013, from informationweek.com.

Three risks of deploying payment kiosks. (2013, March 21). TIO Networks. Retrieved June 24, 2013, from tionetworks.com.

Trustwave. (2011). Global security report 2011. SpiderLabs.

Trustwave. (2013). Global security report 2013. SpiderLabs.

Verizon. (2012). 2012 data breach investigations report. Verizon RISK Team.

Verizon. (2013). 2013 data breach investigations report. Verizon RISK Team.

Why the MSD security breach matters. (2012, November 12). Fightback. Retrieved June 24, 2013, from fightback.org.nz.