#204 - Shadows and Zombies in the Data Center

[00:00:00]

Introduction to Shadow IT and Zombie IT

G Mark Hardy: Imagine Shadow IT is a renegade team of IT users moving in stealth mode. Agile, but dangerous. In contrast, Zombie IT is a forgotten graveyard of technology, haunting your data centers. Unseen, but just as deadly. Each has its origins. It's risks and it's hidden costs. Hey, let's dive into the distinct characteristics of Shadow IT and Zombie IT, the risks they pose, and the proactive safeguards a CISO must employ to keep the organization's IT ecosystem alive, healthy and Secure.

Welcome to CISO Tradecraft

G Mark Hardy: Welcome to CISO Tradecraft.

G Mark Hardy: Hello and welcome to CISO Tradecraft, the podcast that provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G Mark Hardy and today we have a special [00:01:00] Halloween episode where we're going to talk about two IT killers that lurk in every organization.

Shadow IT and Zombie IT. They may seem unrelated, but both could wreak havoc on your security posture, your compliance efforts, and your overall IT efficiency. For any CISO, the challenge is clear. These lurking threats must be understood, controlled, and eliminated before they drain your organizations of resources, or worse, expose you to devastating cyber attacks.

Hey, CISO Tradecraft is partnering with CruiseCon for what I think is a brilliant idea, a cybersecurity conference held during a luxury cruise. Geez, why didn't I think of that? Usually events like this are reserved for Fortune 100 CISOs, but we've worked a deal for CISO Tradecraft listeners so that you can join us on the Royal Caribbean Voyager of the Seas from the 8th to the 13th of February, 2025.

Admiral Mike Rogers is going to be there, so I won't be the senior officer afloat. But if you want to beat the cold while [00:02:00] doing some killer networking, head over to CruiseCon.com and use the code CISOTRADECRAFT10 for a 10 percent discount to this exclusive event. Come join me. All right, back to our show.

Defining Shadow IT

G Mark Hardy: Let's start first by defining Shadow IT, the unseen killer of the IT department. Shadow IT is when employees provision their own IT resources without going through the IT department, plain and simple. It could be software, applications, services, or even devices. And some people figure, hey, If policy says they don't need a receipt below 75, why not expense 74.

99 for a fandom taxi ride to fund your Amazon bill? Now, why does this happen? If someone's in a hurry to get a job done, and the provisioning paperwork takes way too long with IT, it's viewed as taking the initiative. The problem is that if someone increases our attack surface, and IT doesn't know about it, What's going to happen [00:03:00] when something goes wrong?

Chances are, you'll get blamed. Now, for example, let's say your company bans the use of ChatGPT because it's worried that employees will upload sensitive data into it. But there's always an employee who thinks that the policies are, for everyone else. And so despite management saying, no, here's what they might do.

Instead of using their corporate laptop, They'll write a sensitive message or email on their personal phone or laptop and then upload it to ChatGPT to make it sound more professional. And next, they'll take that professional version, copy it into Gmail, email it back to their work email address, copy, paste it and send it off to a client.

by doing this, the employee has bypassed the organization's web proxy block on ChatGPT to gain access to the tool without the IT department being any wiser. See, ultimately, Shadow IT is going to arise from a number of reasons. One of them is, of course, a desire for speed and flexibility. People, [00:04:00] business units, get frustrated by a slow approval process.

They'll just go ahead and adopt a third party app to meet their needs instantly. Also, there's a widespread ignorance of risk involved. Employees lack the awareness of the security implications of using unapproved tools or devices that

will bypass the corporate safeguards. Also, we're in an era of remote work and BYOD.

This explosion with all the bring your own devices and the policies have really empowered employees to, adopt personal apps and software for work processes. And depending upon how you set things up, you might not want to have that deep of a control over a BYOD device, because then when something goes wrong at home, your IT department is fixing it.

And you really don't necessarily want to have that. And then lastly, the software as a service explosion because with the rise of cloud based SaaS tools, employees can sign up for services in seconds without any IT department intervention required.

Risks of Shadow IT

G Mark Hardy: So the real risks of Shadow [00:05:00] IT really start with data leakage.

If you're using an external app like a Dropbox or Google Drive to store sensitive corporate data outside of a secure environment, this can create a potential leak or even a breach. A Gmail sent folder could have a plethora of information that would make your blood gurgle if you realize just how much sensitive stuff was there because employees have been using their own private accounts.

Also, there's security gaps. Shadow IT is going to operate. Under the radar, making it difficult for security teams to enforce corporate security policies like encryption or multi factor authentication. It creates some compliance nightmares. Unauthorized apps may process sensitive data in ways that could violate your regulations, such as GDPR, HIPAA, PCI DSS, and so on.

That can expose your organization to significant fines. There's integration issues. Unapproved apps rarely are going to integrate well with official enterprise systems. You'll have fragmented data, [00:06:00] inefficiencies, operational bottlenecks, and possibly even media that's being used to transfer from A to B that gets left around with sensitive information.

You get an increased attack surface. More apps, more devices, especially ones that are unmanaged, mean more points of entry for attackers and cyber criminals. Shadow. It expands the attack surface, making it harder to secure your organization, and then you also get a surprise outage. What happens to a Shadow IT system?

After a while, people get used to it and if it's any good, they'll incorporate it into their daily workflow. Now, what happens when the employee who sets it up leaves? That monthly taxi receipt stops getting submitted for reimbursement, and the cloud service provider sends a few warnings the bill isn't getting paid, but not to IT, but to the personal account of the employee who's already gone.

Eventually it gets disconnected due to non payment, and then some critical business process breaks. You get called in, and you have no idea [00:07:00] what's going on until you spend a whole bunch of time trying to get someone to fess up and figure out what's going on. So the bottom line is that the true danger of Shadow IT is that it Thrives in secrecy.

It erodes a central IT's team ability to protect, monitor, and manage the organization's digital footprint. Unseen, it grows, quietly increasing risk until a breach or data leak brings it painfully into the spotlight. Having a little bit of fun with this Halloween episode, so let's stay with it.

Introduction to Zombie IT

G Mark Hardy: We'll look at our second killer, Zombie IT, the ghost of systems past.

Now, Zombie IT, consists of outdated, forgotten, or even underutilized systems and applications that still remain active in an organization. These systems may once have been critical, but since they've become unused or even obsolete due to upgrades, replacements, or even just lack of ongoing maintenance.

And yet, despite this irrelevance, they continue to consume resources and expose the [00:08:00] organization to hidden risks. How does Zombie IT arise? From legacy systems, C organizations will tend to move on to newer technology without properly decommissioning. The older systems. And you leave these relics running in the background.

For example, someone wanted to decommission a server, they filled out a ticket, but for some reason never got acted on. Nobody followed up. Or they might have filed the ticket to decommission the server, but they forgot about the special firewall rules, and the DNS entries, and the load balancers, and all the other things that were set up for that didn't get killed off, that still left some vulnerabilities now open when somebody realizes, hey, there's a big hole and nobody's using it.

Mergers and acquisitions. Are another way we get Zombie IT. When companies merge, you're going to inherit a legacy system. Potentially it's not fully integrated. It's not properly retired. You get some orphaned IT infrastructure. And a lot of these will have sparse or missing documentation or none at all.

And it's easier to just leave it [00:09:00] running, rather than risk breaking something. Also, inadequate IT governance. Without a robust process for asset management, organizations will lose track of aging systems, which will fall into disuse, but they'll still be functional and operational. It's just that nobody's paying attention to them.

And cultural resistance. Some teams may resist decommissioning legacy systems out of fear of breaking something critical, or because of a, if it ain't broke, don't fix it, type of mentality. All those things could combine to create Zombie IT, which results in these risks.

Risks of Zombie IT

G Mark Hardy: Unpatched security vulnerabilities is probably number one.

These forgotten systems are rarely patched or updated, or the vendor has stopped issuing patches and updates. leaving them ripe for exploitation by attackers who are seeking easy access to your network. And in addition, they may grant lateral movement through these ancient permissive firewall rules or overly broad permissions that [00:10:00] never got deprovisioned when this system was supposed to have been shut down.

We've got hidden costs because Zombie systems continue to consume resources. Whether it's electricity, or storage, or maintenance time, but that doesn't provide any business value. It creates data privacy risks. If a Zombie IT system stores or processes sensitive data, it might fall out of compliance with current regulations.

You don't know about it until you get dinged. with a penalty or a data breach report, and then you have to go settle that one up. Creates operational inefficiencies because as these systems go unnoticed, they introduce inefficiencies, bottlenecks, they could drag down your performance, they add unnecessary complexity to your IT management.

Overhead in terms of having to pay for processing and virtual machines that are still running and running and every month to get a bill for it. Nobody really knows what it is, but it's not worth the time to pull the ticket. Bottom line, your

Zombie IT is a [00:11:00] drain on your resources and it's a ticking time bomb for cyber security.

Their very existence is a testament to some form of disorganization and lack of a proper IT lifecycle management process and worse. They usually go unnoticed until it's too late, until the breach exposes this vulnerability or an audit reveals that you're non compliant and you get a finding.

Shadows vs Zombies Comparing Shadow IT and Zombie IT

G Mark Hardy: So let's take a look at these two side by side.

Shadow IT, Zombie IT. The source of the threat in Shadow IT. is often because it's initiated by an employee who's in a hurry. as compared to Zombie IT, which is a result of a forgotten or obsolete system. Now, what's the visibility of Shadow IT? It's designed to, hide in the Shadows. It's hidden from IT oversight, but it's usually being used actively. As compared to Zombie IT, which exists, but it's been ignored or forgotten. It may be visible, but nobody [00:12:00] has validated that it's still a requirement. When was the last time you did a zero based review of everything you got in your IT shop? All the apps and things like that. You might be surprised what you find out.

From a lifecycle perspective, Shadow IT, these are active tools in unauthorized use. So you have no lifecycle management whatsoever. And on Zombie IT, they are inactive or obsolete. They may have no further updates. They may have no patches. But it's still operational, which means you're running these systems that have persistent vulnerabilities.

Understanding the Risks of Shadow IT

G Mark Hardy: Your primary risk of a Shadow IT is data leakage, integration problems, compliance, and I would submit also, interruption in business process once the person who has been funding the Shadow IT moves on, quits, leaves, whatever, and nobody pays the bill and the thing disappears overnight. As compared to Zombie patching or updates.

There's inefficiencies in their hidden costs. Shadow IT [00:13:00] exists for people who want speed, agility. They're trying to avoid the IT red tape, and they just say, Get er done, but over on Zombie side. It exists because of poor

decommissioning practices, lack of tracking, or not being able to do a good solid inventory.

Comparing Shadow IT and Zombie IT

G Mark Hardy: And lastly, if we take a look at the idea of Shadow IT, that's created by individual employees or business units or somebody who just wants to get something done. As compared to Zombie IT, which has been created probably by the IT department, but because of poor management practices, it continues to persist and it gets funded.

and it remains a vulnerability. So both the Shadow IT and the Zombie IT are going to grow from a breakdown in organizational processes, whether it's the inability to meet user needs quickly, Shadow IT, or the failure to decommission outdated systems, Zombie IT.

Antidotes for Shadow IT and Zombie ITAntidote to Shadow IT and Zombie IT

G Mark Hardy: Okay, what is the antidote to to Shadow IT and Zombie IT [00:14:00] as a ciso, you have to adopt a holistic, multi-layered approach.

Meaning it's not about reacting to problems, but you want to be proactive. You wanna build a resilient IT framework that is gonna balance both speed as well as control. And so from a perspective of IT governance for Shadow IT, we want clear. Easy to understand policies for acquiring and using new technology.

Get the friction out of that process. Make fast, flexible approval pathways available, so it'll avoid the appeal of Shadow IT, and have management enforce some consequences for violation. And on Zombie IT, you want to have a rigorous IT asset management, or ITAM process, that's going to track the entire lifecycle of systems, from deployment to decommissioning, and ensure there's a clean hands off process When you hand over things from retiring an old system so you know that the data has been moved over, if it's still useful, into a new system and the old system has been shut down, sanitized, and you've been [00:15:00] validated.

Automation and Monitoring Solutions

G Mark Hardy: You can also do automation discovery tools. For Shadow IT, how about a cloud access security broker, a CASB? It can monitor your cloud app usage and provide real time visibility into unauthorized services and combine this with user entity behavior analytics or UEBA to flag unusual software usage. For the Zombie IT, how about automated asset discovery tools and configuration management databases, CMDBs, to continuously track and report on all systems and flag those that are dormant or nearing end of life.

For action. And then take those actions.

Security Monitoring and Auditing

G Mark Hardy: We can do security monitoring and auditing. For Shadow IT, we can perform continuous audits of cloud and network activity to catch unauthorized tools before they proliferate. Data loss prevention, DLP solutions, can help you prevent sensitive data from being stored or exfilled or sent from unauthorized locations.[00:16:00]

And on the Zombie IT side, conduct regular system audits. Identify. underutilized or obsolete systems. Schedule and enforce regular security patching and decommissioning procedures for legacy systems. Remember, I talked about doing a zero based review. Many years ago, I had worked with a financial institution and the bank, now this is way back when, you'd print things out on a green and white paper and a big fan fold stuff, And they were generating hundreds of reports every week, if not thousands.

Spectacular amount of paper was being consumed back in the day. And so new head of IT came in and said, I'm going to do basically a zero base review. What we're going to do is we're going to go out and have people, we're just going to take a bunch of these things and just not send them out. And if somebody calls up and complains, Hey, where's my Monday report?

We send it to them right away. So they printed them and they were ready to go, but they didn't deliver them. Over 90 percent of those reports, nobody [00:17:00] complained about. The ones that people needed, they got to them and they kept them on a production system. Everything else they just deleted and nobody cared.

Now, it's a little bit playing with fire when you go ahead and withhold something. And today, in our instant on immediate communication session, maybe I don't know whether you hold up an application or a login, pop up a screen on it and said, Hey, if you still need access to this, call IT.

Awareness and Training for Employees

G Mark Hardy: How about awareness and training for employees?

For Shadow IT, you got to educate your employees on the security risks of unapproved apps. Make IT an enabler, not a bottleneck. Streamline your process to get new tools vetted and approved and running. For Zombie IT, you want to train your IT staff. and the proper decommissioning practices and ensure they understand the long term security and cost risks of leaving legacy systems running unattended.

Regular Compliance Reviews

G Mark Hardy: How about regular compliance reviews? For [00:18:00] Shadow IT, you want to ensure that all systems are in use, including Shadow systems. Comply with regulatory requirements. If they don't comply with regulatory requirements, then you can't use them. And then perform routine assessments to find these non compliant services and weed them out.

For Zombie IT, you want a formal review of legacy systems to assess their ongoing compliance with regulatory standards. Again, this, go ahead and stop sending it and see if anybody notices. It's a little bit risky, but I've seen it done. And flag systems for decommissioning if they cannot be secured. And that's a real issue.

I just read, yesterday, I was out in California, as you can tell I'm back home today, that, San Francisco is paying something like 210 million to move out of five and a quarter inch floppies for their muni system. They said it keeps working, it works fine, but they're running out of people who can manage this archaic type of a system.

So it's one of those things that if it works, don't fix it. It's been going from the [00:19:00] nineties to the thousands of the tens of the twenties, and yet it's still there. And now it's going to cost them nine figures to get rid of floppy disks. No, I liked a bit on that project. I bet I could do it for eight.

Lifecycle Management Strategies

G Mark Hardy: And lastly, lifecycle management. For Shadow IT, we'll create an approval process that'll balance speed with security. They said enable rapid integration, new technologies. but enforce visibility and security measures. Let

people know that you're there to help, you're there to empower them to get their job done.

They don't need to go around IT, but then make it so it's not difficult to do. And for Zombie IT, you want to have very strict protocols for end of life systems. Implement processes to retire this old infrastructure on time and ensure a smooth migration to modern platforms. You probably floppies writing mission critical type of a communicator.

transportation in a major metropolitan area, even though it still works.

Summarizing the Threats and Solutions

G Mark Hardy: Okay, so how do we summarize this? At [00:20:00] first glance, Shadow IT and Zombie IT might seem like a kind of a quiet passive risk. Yeah, okay. But both have the power to destabilize your organization's IT environment. Shadow IT is going to undermine your security from the inside.

Zombie IT is going to weaken your foundation by leaving outdated, unmanaged really systems in place. The solution isn't to stifle innovation or hold on to the past. You have to create a robust governance framework that's going to promote agility while ensuring that every system, new or old, is accounted for, secured, and compliant.

Go through and do a full system inventory. If you haven't done one for a while, Do it. You'd be surprised what you find. And then figure out ways to look for things that you didn't think were there. That'll spot the Zombie IT. But for go ahead and your Shadow IT, how do you find what's being used? Look for applications that aren't supposed to be installed, but are installed on your devices.

Look at your firewall logs, look at your communications, your DNS logs to see [00:21:00] where are people going. Are they going to software as a service tools? Have you said don't use LLMs, but people are using LLMs? And if you don't define your rules too quickly, oh, don't use ChatGPT. Okay, great. So I'll go ahead and use something from Anthropic.

Figure out how the rules are going to work, but figure out why your employees are doing what they're doing in the first place and find ways to enable them and empower them to get stuff done. I think AI, we're at the cusp of that. We've done a couple episodes on it. I'm going to do a whole lot more, I'm sure, because I'm learning more about it.

I just, Find there's some spectacular opportunities there for efficiencies, for improving the quality of products and things like that. someday I might be replaced by an IT bot just chatting away, but hopefully not for a while. In any case, what you want to be able to do is work with your business units.

Spend some time understanding what is it you need to accomplish your mission today. And what is it you think you're going to need to accomplish your mission [00:22:00] tomorrow? Work with them to identify applications, tools, services that are going to allow them to reach those goals in a manner that you can manage and oversee.

See, if you face both these threats head on, both Shadow and Zombie IT, as a CISO, you can transform your organization into one that will foster innovation. while still having rock solid security and operational efficiency. The problems won't disappear, but with the right strategy, you don't have to live with them either.

Final Thoughts and Call to Action

G Mark Hardy: So we hope you've enjoyed listening to this Halloween Week episode on Shadow and Zombie IT. Now, hey, if you learned something, please do us a favor and share it with a work colleague or post it on social media. And if you like the content, please subscribe, not just to our podcast channel, but also on YouTube.

Or even sponsor a future episode if you're a vendor. We can get you great exposure. Plug, right? I want to share with you a little secret. We got different content on different platforms. So if you've just been listening to CISO [00:23:00] Tradecraft, you're missing out because each week we post a weekly substack newsletter with images that you're not going to see anywhere else.

On LinkedIn, if you follow us on LinkedIn, we're going to share content and interesting articles during the week. And we get some spectacular feedback and the comment sections are great. So you can read what your peers are saying as well. And if you like short clips, we even have little YouTube shorts.

And guess what? Apparently I'm on TikTok as well. So you can look for a couple of those little short videos to check us out. anyway, thanks again for tuning in. And you want to stay safe from all those Shadows and Zombies that are out there. And don't forget to check out cruisecon.Com and use your CISOTRADECRAFT10 discount code and join me out at sea next February.

Until next time, this is your host, G Mark Hardy. Stay safe out there and trick or treat.