Heather:

Welcome to The Hurricane Labs Podcast. I'm Heather, and today we're going to follow up on the cybersecurity concerns related to Russia's war on Ukraine. Now, since his executive order on cybersecurity last year, President Biden's administration has been highlighting the need for American organizations to strengthen their cybersecurity stances. In light of Russia's recent activity, Biden's administration has been pushing this issue even harder, saying it's become an even more pressing national security issue as nation state actors out of Russia could begin targeting American businesses. On Monday this week, March 21st, President Biden issued a statement that included the following segments: "Today, my administration is reiterating those warnings based on evolving intelligence that the Russian government is exploring options for potential cyber attacks." He continues on to say, "If you have not already done so, I urge our private sector partners to harden your cyber defenses immediately by implementing the best practices we have developed together over the last year. You have the power, the capacity, and the responsibility to strengthen the cybersecurity and resilience of the critical services and technologies on which Americans rely. We need everyone to do their part to meet one of the defining threats of our time. Your vigilance and urgency today can prevent or mitigate attacks tomorrow." Note that we have included the link to the full statement in our resources. In response to these growing concerns, I have Hurricane Labs Director of Security Operations, Josh Silvestro, here to discuss with me what some of the best practices are and what you can do to strengthen your organization's security stance in these short and long terms. Thanks for joining me, Josh. I know things are a little bit crazy this week, so I do appreciate you taking the time.

Josh:

Yeah, absolutely happy to be here.

Heather:

So what steps should organizations take as soon as possible? What can and should be done immediately in the face of what's happening in Ukraine?

Josh:

Yeah. The truth is in situations, not only like this, but pretty much every big event that pops up, it's funny how it always comes back to the core things. There's always a core set of things that everyone should be doing even prior to the threat of Russia to keep their organizations safe. And a lot of those things fall back to looking at your organization outside in. If you're an external party, how are you making your way in? Do you have externally facing services? If so, are those secured? If you have authentication, are you using multifactor authentication in managing login attempts, just to make sure that someone's not brute forcing their way in? I know that Biden had kind of listed and outlined a bunch of things around using multifactor authentication, a password management policy, backing up your data, which again, his list is core fundamental cybersecurity practices. So not only should you look at the obvious things around the services, how they're hosted and where you might be vulnerable, but what's your fallback plan? The truth at the end of the day, there is no perfectly secured organization. The software, the hardware, even people are all weak points in organizations. So what do you do when one of those things fails and the other security controls can't compensate and you potentially have compromises and start losing data. One of the first things you should do is look at your backups and have a plan in place for restoring those. One of the things that everyone's guilty of at some point is testing those backups. It's not uncommon for an organization to have a fantastic backup system. In a moment of need, they go to restore data and it's either corrupted, the backup doesn't restore as they

expected, or things just don't go according to plan, which really causes a lot of headache, causes additional downtime. And if you're anyone that's in charge of productivity or finance, you know those moments that are down can be really detrimental to a business. So you should be testing your backups, making sure everything's in place and run through some drills on how those will be restored as well as using actual situations to restore the data again, and invalidate the process and the integrity of the data. One of the things that Biden had recommended was tabletop exercises, which I think are really great. We do them here internally at Hurricane Labs, as well as we have clients that go through tabletop exercises and actually will include us on those as a Splunk resource. So as they're running through some drills or some practice scenarios, they'll say, "What can we find related to this in Splunk?" Which then they call on us and we pivot into their Splunk instance and do some threat hunting or pull the related logs to help validate the tabletop exercise. One thing of note, and I wish I had a name to it, but I think it's actually a really great product, you used to be able to get them at DEFCON, there's even companies out there that make a tabletop exercise security card game, where essentially you flip a card up, it gives you a scenario and you have to act through it. Even something like that is just a really good guiding hand in kind of running through some tabletop exercises or again, look at what externally facing things you have, where you're truly, truly vulnerable. And then go through tabletop exercises on public web server being hacked. What would your response be? An account is compromised. They bypass multifactor. What's your response? Running through those things is going to make sure in a moment of panic that everyone's kind of got a cool head and knows exactly what needs to be done.

Heather:

Is that card game you're talking about, is it Backdoors & Breaches?

Josh:

Actually, let me see. I think it was within reach, but I just couldn't see it. Yeah. It's Backdoors & Breaches.

Heather:

Yeah. I bought that just so I can like learn the language and some of what it might look like, and it's actually an entertaining game. It's actually pretty fun too, in addition to it being a learning opportunity for me, it was actually pretty fun to play.

Josh:

Yeah. Well, the fun thing about it from an actual, real world use is it's extremely common for firewall admins, for example, to be like, ooh, let's focus on firewall stuff, but that's not how the world works. So the card game doesn't really give you a choice in the scenario, more or less, which is kind of why I think it's a really good resource.

Heather:

So as far as learning opportunities go we know that, like you said before that people are a source of vulnerability for companies with phishing and social engineering. So what can and organizations do to help make sure that their employees are resistant to being susceptible as far as cybersecurity issues go?

Josh:

Yeah. Some of the most common methods of training employees stem from just internal meetings, whether that's depending on your business needs, quarterly, biannually, annually, where you kind of get

together, talk through company policies, kind of reassure the very basics of even things like, hey, when you're walking in a front door, especially if there's a badge reader, do not let someone walk in behind you. That happens when people go through physical pentests, one of the biggest ways that people try to sneak into buildings to test security is by tailgating and having two cups of coffee in a hand trying to say, "Hey, hold the door for me." So talking through those things and kind of explaining why they're important and really drilling those in, helps establish a good physical security. But then also extremely common is doing phish testing where an organization will send out phishing emails that try to test an employee's ability to detect and report the email. So for example, an employee receives a fake phish email, they report it and they'll actually get a notification like, "Hey, good job. You caught this. This was a company phish test." And it's reported back. On the other hand, if you don't catch it or you click on a link, it's logged somewhere and then you can have an employee you like immediately enrolled in some training explaining what they didn't catch. And these things are always changing. So a recurring set of training, a lot of people tend to do phishing, I think monthly or quarterly is the most frequently I've seen recently, just where you can constantly keep testing employees and it's not to knock your employees or make them feel like they're not capable of catching these things. But you'd rather catch them missing an opportunity to report a phish or falling for a phish than to let an attacker actually take advantage of that as well.

Heather:

All right. So what about over the long term? What steps can we at least start taking now to improve our security stances in the future?

Josh:

Truthfully, when you think about how people typically infiltrate an organization, usually the first is people. People are a weak link. So again, go back to training. Training's not a one and done. That's just something that should continue for the life of your organization and should adapt and evolve as threats adapt and evolve. On the other hand, when it's not an employee being phished, it comes back at policies and weak things like firewall rules or networks that aren't properly segregated, which are again, fundamentals. And as organizations grow, sometimes it's hard to kind of redo things and go back to the fundamentals. But if you start building them in, as you continue to move forward, it makes it kind of easier to go back retroactively and fix those things. And lastly, software, still kind of falls on the process of humans typically being the weak link, but no software's written by humans. They're not perfect. They make mistakes. So if you have the ability to control some of what's being built, especially if you're doing internal scripts, he helps a ton to have someone with security knowledge or a pentester review those scripts, provide best practices or things that they see could be a weak point and fix those. Really want to make sure that everything you're doing from your training of your people, to the products, to the networks, to the processes you build out, have security in the mind from step one, which will make your organization significantly more secure. On top of building out processes with security in the mind from the start, something you should do along the way, no matter how much security is involved, is continually test those processes. Like I said, you could have someone review code that you write internally, but also you should be bringing in a third party that's not really familiar with the organization to do regular pentests. Throughout the year, your organization might change, new network products are installed, new software's pushed out. And as those things change, you should be retesting your network. And that's you usually where having a pentest group come in and attack your network in a real world situation is really helpful. It's good for them to find the weak links, report them back to you and then you can make those changes and you should retest. But at a minimum you're aware and once you've made the changes, in theory, that's closing one avenue for compromise in your organization. So using

pentesters is great. You should also be doing regular vulnerability scanning, which if you're not familiar, is typically a tool stood up within a network where externally that scans it and looks for easy wins. Maybe it sees a service on a firewall running and says, hey, that model of firewall in that service is vulnerable to this. You should patch it with this software. It's a good way just to make sure things aren't slipping under the cracks and you're not leaving easy avenues of compromise open, that can easily be detected and repaired using something like a vulnerability scanner.

Heather:

All right. Well, are there any last points or recommendations that you want to offer?

Josh:

I guess the last thing I would say is, especially with this week, big in the news is the Okta breach. All of the products and services that you have in the organization, if they have a log and it's a security use case, you should be putting those into a SIEM, such as Splunk. The value there is in the Okta case, a lot of people were surprised to find out that they only hold logs for client instances for 90 days. That means if something happened 91 days ago, you really don't have access to it. You can't validate it. And if it's a long term compromise, you can't track it back properly to see where it all started. So ingesting those log into something like Splunk, not only allows you to retain them longer, but allows you to kind of tie a multitude of solutions and logs back to kind of unified timelines so you can understand what really happened in your network. And I think when we're talking about the Russia and Ukraine potential attacks coming, this is extremely important. If there's some compromise that happens and you have reason to believe it's tied back to Russia as more attacks inevitably happen and companies disclose what happened, how it happened, the IoCs, you can then search your logs, looking back over whatever timeframe, six months, a year or longer looking for those IoCs so you can find the initial start of a compromise and tie them back. If you're lucky enough to not find those things, then even more importantly, you can run a correlation search or an alert that will constantly look through your logs for you. And when it finds those things, detect them, alert your SOC team or your network team, or whoever's going to handle your incident response and can take action immediately. At the end of the day, how fast you detect and react is what keeps the compromise short and limits the damage to your environment.

Heather:

All right. Well, thank you very much for are taking some time today. Like I said, I know this week's been just a little bit crazy, so I very much appreciate it.

Josh:

Yeah, absolutely. I'm always happy to help.

Heather:

And that's all for now. So be sure to check out our links where we shared a number of resources that we touched on here today. And until next time, stay safe.