Eliezer Kanal: Welcome to Cyber Talk. My name is Elli Kanal, I'm joined today by Matt Butkovic, and we're going to talk a little bit about some of the current events going on within cybersecurity. As today happens to be directly, squarely in the middle of the flu season, and you can probably hear me talking about that, why don't we get started a little bit talking about some of the cyber-hygiene practices that we're seeing coming out, especially with some of the attacks that were happening in 2018.

Matt Butkovic: Sure. So let's talk about the concept of hygiene. So hygiene--physical hygiene in the medical profession specifically, right? So everyone can generally agree that washing your hands will help prevent infection, but at one time this was a controversial topic as well. In fact, there was a Hungarian doctor named Ignaz Semmelweis, who in the 19th century promoted the idea that washing hands would reduce infections in his patients, and he was widely decried by his fellow doctors, and it took nearly 80 years for his ideas to be adopted. But as we know, it's a basic tenet of the medical profession now-- you must wash your hands and not allow contamination between patients. Cyber-hygiene is a much newer concept. The idea is what is the minimum set of things we can do to reduce the changes that we have some bad event, right? So malware or some other exploitation. I would argue just like it took quite some time for the medical profession to adopt physical hygiene, it's taking time for an organization to get comfortable with the idea of cyber-hygiene.

So you also find that, although for now hundreds of years we've known washing your hands helps reduce the chance of infection, many doctors still fail to do that-- a shocking percentage, right? I saw an Australia survey from 2016 that 36 percent of doctors in this given hospital did not adequately wash their hands between patients, right?

So, why do I tell you all this? I think we have to adopt the mindset that when we establish the basics and we focus on the basics, it takes diligence to reinforce the importance of those basics. So I'm really sorry to see you're suffering from a cold, and to kind of tie the conversation together, Elli, I think we could give folks today an understanding of things they can do at a basic level that helps prevent some of the atrocious things we saw in 2018 in cyber.

Eliezer Kanal: Sure. I know that some of the stuff that I've heard about at least as good practices-- you have to choose strong passwords; a lot of people are now pushing these password managers; we have a lot of concepts that you want to use two-factor authentication. Are there certain ones that you want to portray that, "Hey, these are the things we've really seen being problematic in terms of causing attacks, or causing other kinds of data loss"?

Matt Butkovic: Yeah, there's many lists out there. So I'd point to the Center for Internet Security's list, their cyber-hygiene list. The CERT Resilience Management Model, we have a cyber-hygiene list listing the essentials. The Australian Signals Directorate has also done a really good job of creating that list. You mentioned passwords or credentials, right? So I'm thinking about notable events in 2018. If I think about, for instance, the Under Armor breach that we saw, we now know that passwords were stored both in a very strongly encrypted way using BeCrypt, and then a less strongly encrypted way using SHA-1. To me, that's an example of taking your eye off the fundamentals, which is: Why don't you have a comparable level of encryption for all passwords?

Also prompting the conversation, do we need to go beyond simple passwords for credentialing or do we need to adopt a two-factor approach, for instance?

Eliezer Kanal: Sure. And one of the things, as you're talking about that, there's a lot of-- as a user-- let's say I'm just some guy trying to use my company network or I'm someone trying to use an online service, or even just something temporarily to share something with a friend, I don't have control over the kind of infrastructure that they're going to provide for me. So is there anything that I would want to do to make sure that however I'm using the service, it doesn't really hurt me in the long run?

Matt Butkovic: Yeah, I think there's a concept of fit-for-purpose, which is the first thing a person, and more of an organization should do, is to determine the requirements to protect that information, and this fits directly into cyber-hygiene. Step one: Know what you have. Understand the nature of the assets you operate. How are those assets used in the organization? Once you've made that list of the essential things that you do and the assets that support them, then really think through the protection requirements, and this is going to vary. So Elli, if it's a recipe you put in the cloud, it's different than information related to national security, for instance, right? But in both cases, you can articulate a specific risk scenario and a specific set of requirements to protect that information.

Eliezer Kanal: And going back to the doctor example, it's really critical that a surgeon, prior to doing surgery, washes his hands and uses all the soap and uses everything he needs to.

Matt Butkovic: The techniques will vary based on the criticality and the nature of the threat, right? So in the case of infection, you're describing sort of-- in the medical profession and also the diligence you apply is dependent on the context, and the same thing applies in cybersecurity, right? There is no sort of one-size-fits-all. With that said, I think we've been striving for a long time, and cyber-hygiene is an articulation of, is: What is that minimum baseline? What are those set of practices we expect everyone to do? So if you're using the Amazon cloud or you're trusting your credit card with a very small vendor, are they employing the same concepts to protect your information?

Eliezer Kanal: Right. To kind of move off of passwords for a second and talking about the protections there, so there's been a lot of ways that data has been attacked in the past. We talked a little bit about passwords. I know one of the ones that comes through is phishing, and when you're doing a phishing attack, or when someone's trying to execute a phishing attack, they're not so much relying on an insecure password or even insecure data; they're trying to bypass all those protections and access the data in a second way. How would you say people should be protecting themselves against that?

Matt Butkovic: So phishing remains one of the most effective techniques that attackers use because it plays on human frailty, right? No matter how much you train your workforce, unfortunately a certain percentage-- it might be small-- will still probably fall for that payload, right? They'll click on that malicious attachment. It's sort of strange when I think about it. When I think about the usability of computing, it's one of those issues where we tell the user something really dangerous can happen, and we give them very few really sound technical safeguards. We basically say, "Be smart about things and don't click on stuff that looks dangerous." Right?

Eliezer Kanal: Right.

Matt Butkovic: So, step one: Don't click on things that look dangerous, right? But beyond that, I would advise that organizations and even people in their individual lives should think hard about the way they consume email. If it's not from a trusted source, if it's not valid, in some way you readily recognize, "Don't click on it." Right?

So let's talk about phishing. Phishing just doesn't affect the theft of credentials for individuals, it doesn't just affect the exfiltration of credit card data, it's also-- there's good evidence it's affected critical infrastructure, right? There are examples now where control systems have been compromised or it's believed they've been compromised as a result of a phishing threat vector.

Eliezer Kanal: That's interesting. And as things get compromised and as people are getting access to it, it just makes it that however strong all the protections you may have in place, those are all bypassed, and there's really-- all the work you put into it, just because this person was able to get the phishing through-- all that was for naught almost.

Matt Butkovic: Right. So think about it this way. We're talking about what the essential minimum practices are, right? You've conducted these elaborate defense, right? You've spent a zillion dollars on stuff that hangs off the network, right? You've gone to RSA and you bought all the boxes with blinky lights that are going to make you safe. And then someone gives away the key to the door lock that allows them to steal your data with phishing. So it's really a vexing problem, because it feels like we should have a better technical safeguard, and we really don't. Now, there are smart things you can do and certainly products that help, but I think this will remain, at least in the near term, a real worry for all types of organizations.

Eliezer Kanal: Right. So one thing which I think a lot of people tend to have issues with is the fact that no matter-- I like the term you used there, "boxes with blinky lights", because it really kind of fits it. You have this big room filled with boxes of blinky lights, but those don't really work-- they're only as strong as your weakest link, which tends to be the person using all the software and hardware. So to that extent, are there best practices for how you educate the people, "Hey, be careful of things about phishing, be careful of plugging in USB drives, be careful of all the small stuff that tends to break these networks down"?

Matt Butkovic: Yeah, I think training the end-user, right? So educating the end-user in cybersecurity has a place. But I think-- and this is a somewhat controversial opinion potentially-- which is we should look to other disciplines, right? We should expect that a user of a computer will look and feel and operate like the user of an automobile or a toaster, right? There's things that are rational to say don't do, and things that are implicit you shouldn't do, and things we know that are just the abuse case, right? So I think that's one thing I'd add there.

Talking about-- and I think we've coined a term, which is "boxes with blinky lights"-- I would argue we're awash in boxes with blinky lights and most organizations have racks full of last year's boxes with blinky lights that don't blink as brightly anymore. They don't twinkle like they used to. I would argue it's an absence of process and planning that is holding us back in many disciplines, right? If you don't tie these things together, if you don't look at cybersecurity as an engineering problem, how do you ever truly articulate the requirements for things, right?

Eliezer Kanal: That's interesting, and as you were speaking, it makes me think a little bit about not just the fields of-- you said automobile, but even something like finance. There's been a huge amount of work in the financial field that, "We're going to protect the consumer against people who are trying to get whatever it is they have." And there's been a lot of work, "How do I design a system where even someone who really has no knowledge of finance, and they're just trying to use this system to buy groceries, won't get scammed?" And we've almost put the work on the finance industry much more than on the individual. The individual is protected an awful lot. Is that something that you see? I don't know what kind of practices you expect to be seeing coming out of the general IT and security industry to move that forward.

Matt Butkovic: So I'll offer you this, right? There's an idea in psychology, the paradox of choice, that if I put ten jars of jam in front of you and then I put 20 jars of jam in front of you and then 30 jars of jam, you're actually increasingly less likely to actually select a jar of jam, right? The idea is that by giving people more choices that they don't fundamentally understand the difference between the things they're choosing between, you're actually making their decision-making harder, and I feel like some information systems are giving people that experience, which is there's many ways to protect yourself. Should I hit "Update Now", or should I not click on the link, or do both? It's saying for me to provide my domain password. I don't know what the domain is, but I know what my password is. Should I put it in there? I think the more that we can streamline and reduce the complexity of the decision-making, the better off we are.

Eliezer Kanal: That's interesting, and that comes down both to those who are designing the software, those who are designing the hardware, and those who are trying to put the whole thing together for someone to actually use it. That's a pretty big challenge, I would imagine.

Matt Butkovic: Yeah. So I think the hottest topic right now in any technical sphere is artificial intelligence and machine learning-- I know a topic you think about a great deal, Elli-- and one of the things that occurs to me is that we're still struggling with the fundamentals, we're struggling to determine what appropriate user behavior is. I'm just imagining this future where a very complex algorithm is making decisions by themselves, essentially-- I mean, programmed by people, obviously-- but I'm worried that we're going to create very complex systems of systems where the fundamentals still aren't addressed. I know this is a domain you know quite a bit about. Any thoughts about how we can have assured autonomy? I know that's sort of a buzzword, but how do we create greater faith in AI and ML?

Eliezer Kanal: I mean, so for right now, the AI and ML field is really still in its infancy. The way we try to split it up, there's a huge amount of effort that's been put into designing these really smart algorithms. That was actually done decades ago. So we've had the same general algorithms, the same techniques to do these things for a long time. The problem has been we haven't had an effective way to manage the huge amount of data required to actually gain benefit from these algorithms. So to that extent, we're just entering the period now where we're learning how to use these algorithms with the existing data we have. One of the things that we're learning is that in certain areas, things work really well. So if you go to a modern search engine and you type in, say, "bird" and click on Image, it'll show you tons of pictures of birds because image recognition turns out to be a good problem. But for other areas, it's not quite so clean. So cybersecurity is one area where you want to say, "Find me everyone who's hacking into my network. Find me all unauthenticated users who are trying to get in," or, "Find me someone who's sending me malware." That turns out to be a much harder problem for a whole variety of reasons. So at this point, I think we're still a bit out from really having that be a turnkey solution, to pop that new blinking light box in and go.

Matt Butkovic: So is it fair to say that humans will be in the loop for quite some time?

Eliezer Kanal: I think we're pretty good. You're pretty assured with that.

Matt Butkovic: Right. I mean, no one knows exactly what the point will be, but it does seem to me that, like any new technology, there's going to be this hype cycle, and with AI, it seems like some of the projected benefit is getting ahead of the state of the technology, which is, again, I think a pretty common occurrence. I see this very complicated future, again, where human beings are still human beings, algorithms are doing things that are new and novel and difficult to understand, and we're doing so much of this at arm's length in the cloud, right?

So a third-party-- it's extraordinary if you look at the growth of a third-party doing X, Y and Z for you, right? So this might seem like an overreach potentially in this conversation, but I really think that one of the things we need to reskill folks on is not just AI and ML, but also understanding the nature of third-party relationships, right? How do service-level agreements function to protect you? And I would argue that that should be added to that list of cyber-essentials, which is understanding how to have justified confidence in a third-party, justified confidence in an algorithm, justified in an algorithm operated by a third-party. It all comes down to evidence and understanding the things you own, what they do, and what your risk appetite is.

Eliezer Kanal: And that's interesting. One of the things which we see a lot when we're trying to deploy these AI algorithms is people don't understand what it is they're getting, they don't understand how to assess whether it's performing properly, and they definitely don't understand, when the data comes back to them, what should they be doing with it. Oftentimes they think it's like, "Well, here's the answer." Frequently it's not giving you a single answer; it's just giving you evidence, and then once you're trying to provide and act on that evidence, it's honestly not so easy to tell what direction you should go as far as a decision. So there's definitely a lot of work to be done there.

Matt, thanks a lot for joining me. I really appreciate it.

Matt Butkovic: My pleasure, Elli. Thank you.

Eliezer Kanal: Thank you all very much for joining us, and for more information on our work, please see the website below or send us an email. Thank you very much.

Related Resources

Center for Internet Security

CERT Resilience Management Model (CERT-RMM) Version 1.2

Cyber Hygiene: 11 Essential Practices

Australian Signals Directorate

Why Phishing Matters

AI at the SEI

VIDEO/Podcasts/vlogs This video and all related information and materials ("materials") are owned by Carnegie Mellon University. These materials are provided on an "as-is" "as available" basis without any warranties and solely for your personal viewing and use. You agree that Carnegie Mellon is not liable with respect to any materials received by you as a result of viewing the video, or using referenced web sites, and/or for any consequence or the use by you of such materials. By viewing, downloading and/or using this video and related materials, you agree that you have read and agree to our terms of use (http://www.sei.cmu.edu/legal/index.cfm).
DM19-0070