Micro Focus Reimagining Cyber Kate Scarcella Edit V1

Fri, 9/17 3:33PM • 16:41

Blog | Listen

SUMMARY KEYWORDS

ot, devices, iot, kate, technology, securing, security, iot devices, operational, electrical grid, cyber, reimagining, industrial control systems, attack, cybersecurity, environment, iot security, security controls, called, area

SPEAKERS

Rob Aragao, Kate Scarcella, Stan Wisseman

Kate Scarcella 00:03
I often talk about 'the internet world is colliding with the industrial world, and that the data is no longer is isolated. And in fact, it's being aggregated and being analyzed in the cloud'. So everything has become much more public and available. And the ramification of this is that the attack surface has become immeasurable, and as a direct result, we see ransomware that is now a $6 trillion industry. And in fact, you know, we now even have ransomware as a service.

Rob Aragao 00:40
Welcome to the "Reimagining Cyber" podcast where we share short to-the-point perspectives on the cyber landscape. It's all about engaging and casual conversations and what organizations are doing to reimagine their cyber programs, while ensuring their business objectives are top priority. With my co-host, Stan Wisseman, Head of Security Strategists and Robert Aragao, Chief Security Strategist, and this is "Reimagining Cyber". Stan, Who do we have joining us for this episode?

Stan Wisseman 01:12
Rob, our guest today is Kate Scarcella. Kate is the Chief Security Architect with CyberRes, and has been in technology for over two decades. And she has a primary focus on cybersecurity and specifically around the area of the National Information Infrastructure, as well as securing operational technology or OT environments, and the Internet of Things or IoT. Kate, is there anything else you'd like to add on your background to share with our listeners?

Kate Scarcella 01:42

The only thing I would add, Stan is that I did my master's thesis on securing the electrical grid for North America at a school where the curriculum was developed by the DoD and NSA, which at the time, there was less than a dozen schools that were participating in this program. As I look back, I truly get amazed at the growth in cybersecurity.

Stan Wisseman 02:03
That's so true. I mean, we certainly have seen crazy growth. I've been doing this for a long time as well. And it's, you know, one of the areas that we're seeing this in, right, is the explosion of internet connected devices, or IoT, and just the security of those devices. You know, we're using IoT in all kinds of different ways, whether being consumer electronics and enterprises in the industrial world. I know you've been focused on this for quite a few years. Why do you think IoT security is so critical?

Kate Scarcella 02:41
When we talk about the explosion of IoT devices, we're actually talking about 14 billion devices that are connected today. So how do we protect 14 billion devices that are not only a part of the fabric of our society, but are fabricated into our lives, as we see with medical devices, for example? While there are a few legislative initiatives that would help us to identify IoT vulnerabilities and threats, we're basically living in what I call the Wild Wild West. It's not unusual in building access control networks known as BACnet to find no authentication. This is serious because smarter buildings are feeding into Smarter Cities, and all you need is just one point of entry. The traditional security controls that we have seen in it are not thought of in IoT. Oftentimes, with IoT, no password authentication is needed. And information, if it is provided, is in clear text. I consider this to be critical.

Rob Aragao 03:48
So Kate, as you just mentioned, are conventional security controls really not as applicable, per se, to solving for IoT security? What with your background, again, you've been doing this for a long time, and very much an advocate for going after the the OT landscape and securing that, but when you look at IoT in general, what's your vision for how we properly secure IoT?

Kate Scarcella 04:11
So, I think the IoT is literally like, like a tidal wave. It's, it's going to change the landscape that we know today. So when I think about trying to solve IoT will be solved through traditional security controls, I do not think so. The reason being is the speed of which IoT devices are being adopted are coming online and are available. So we need to try something different. A great place to start is with an agent on an IoT device. Endpoint Detection Response similar as we have on our laptops and mobile devices. That's, you know, that's the idea behind this. However, in addition to an EDR for IoT, we really need to embrace Artificial Intelligence and Machine Learning. AI and ML, we cannot just have an agent on an IoT device without AI and Ml. The reason being is the amount of data is overwhelming. If the amount of data that we're dealing with today is overwhelming, imagine 14 billion devices and all that data that's coming in.

Stan Wisseman 05:22
So Kate, let's shift over to operational technologies or industrial control systems, which I think is somewhat similar to some of the same challenges, but is a bit different, you know, we do rely on these

operational technology environments for our energy and controlling our water and transportation. And cybersecurity should be essential. Certainly, safety is an aspect of OT that has been embedded into their environment for years. But I don't think based on our conversations, that OT has the same level of rigor, as far as security, as they do on the safety side. And I'm, you know, for our listeners, if you wouldn't mind also just explaining a little bit about what, you know, operational technology is and distinguishing that from it. Because not everybody will know the difference. But if you can do that first and then get into some of the security replications. And that'd be great.

Kate Scarcella 06:31
IT, traditionally, when we have tried to secure it, we've thought about it from confidentiality, from integrity and availability. Now, when we come to Operational Technology, it reverses. And this is one of the biggest challenges that we have in IT is understanding with OT that the devices first need to be available, and they need to always be available, the valves always need to be working. So, as an example, we have valves that can open and close the amount of, you know, chlorine in the water. And everything is very, very exact. And if anything should go wrong, then, as we have seen with some incidents recently, it really does impact us. So, as an example, if you think about, so OT to get back to the point of security, tenants and principles, OT is based on availability, then it's based on integrity, then it's based on confidentiality. So we sort of changed the paradigm and goes upside down. And traditionally, OT environments, and the people who are running the operations have not had good relationships with information technology people because of this, because there's a lack of understanding of the importance of what they do. So with that being said, the OT devices are are often known as Programmable Logic Controllers, what we know is PLCs remote terminal units, safety instrument systems, very, very, very small devices that are extremely chatty. So, as an example, when I was doing my thesis with the electrical grid, I would ask people, just let me hear the start and stop of a PLC of a programmable logic controller on the electrical grid, that would make me very happy. And from that, I was able to understand as I, as I got the log into a SIM, I was able to understand that something's happening here in the transmission management system, in the electrical grid. That was pretty cool. Back in 2006, so that was like, Whoa, this is amazing. So, um, and it went from there. But now today, what do we see? What we see is that these devices are legacy and I really mean legacy. Some of these OT devices don't have any memory on them at all. And so you really can't put an agent on them. However, on the other side, I see what I what I believe to be a disruption in this area, because I see, so these, this is called Brownfield technology, the old devices that are in there that have been in there for a while. However, with new energy, such as windmills and solar, comes greenfield devices. These are much more agile, much more willing to get an agent on these devices. And I truly believe that there will be this disruption. And that's an area that we we really need to start thinking about this now. But it's also important to control the legacy devices. How do we control the legacy devices? We have what's called the Human Machine Interface, the HMI. It's a device that's, that speaks to the device, all the devices underneath it. So this is an area that I believe can help in securing IoT devices.

Rob Aragao 10:48
One of the biggest and most kind of, notable attack in OT, that in the years past was Stuxnet, right, and everything that happened, there really was an eye opener, I think, as a whole. So, think about the attack tactics that are evolving in what's happening in the OT space specific and kind of share some of your perspective on that front.

Kate Scarcella 11:08
What I would say that, you know, when I think about the change, what I believe has changed. When I look back at this and doing the, you know, the history, and I've looked at the history of attacks, is that today, they are more frequent and more costly than ever before. One of the first examples that we have an attack on on OT, happened in 1997. It was a packet switching network, based on at for an airport. So 1997. The next one that we have is in 2000. We see a city's sewage system was compromised. So about every three years, we were seeing an attack and industrial control systems. Then to a now, it has become multiple attacks and industrial control systems in a year, year over year. So that is, that is the difference that I have seen. Yet, I would say that, interestingly enough, that the tactics, the actual tactics have always remained the same. Meaning that when we, when we break down the attack of industrial control systems, it is not unusual. And I repeat that. And I'm saying that it is within a 90% range where the attacks are coming from above, from the IT side. So think about that. So if we can, before they cross over into the OT side, we're actually seeing, seeing that they gain entry, that they do lateral movement that the bad guys are doing lateral movement, that they do privilege escalation, that they run commands that that usual, computers aren't running, justifying that access point into the OT environment, that has been the same. But what has changed is the frequency. And just the cost has just become enormous.

Stan Wisseman 13:31
Okay, in in the past, there was certainly was a lot of effort or perception that the OT environment was segregated from the IT environment, that you really had distinct networks. And even though the bad actors had potentially come in for the IT side, it would be difficult to find that entry point into OT in though in some cases we point out, they were successful. I think what we're seeing now is unfortunately, that convergence, right, between IT and OT, more intentional convergence. And there are ramifications of that, you know. We're blurring the lines. And in some ways, that's to perhaps have efficiencies, right? If you look at the the intent for the business to perhaps make things process wise, more efficient. At the same time, as you're pointing out these bad actors can have easier access then to these target systems on the OT side, is that is that what you're saying? As well as that, that convergence? Is it aiding and abetting these threat actors?

Kate Scarcella 14:46
Absolutely. Absolutely. I often talk about the internet world is colliding with the industrial world, and that the data is no longer is isolated. And in fact it's being aggregated and being analyzed in the cloud. So everything has become much more public and available. And the ramification of this is that the attack surface has become immeasurable. And as a direct result, we see ransomware that is now a $6 trillion industry. And in fact, you know, we now even have ransomware as a service. Yeah, it's kind of hard to believe, but it is hard to believe, isn't it?

Rob Aragao 15:25
Yeah. So Kate, very, very insightful. I think, you know, again, you have a passion for this space. You've, you've been, as I mentioned earlier, a major advocate for many years. I think the reality is that people are starting to pay attention. It makes all the sense in the world, why they should be paying attention, and obviously also different approaches and solutioning that they can actually apply that are

acceptable for them to actually take forward as part of their overall cybersecurity strategy to support IoT/OT environment as a whole. So thank you for sharing all of your knowledge in the space and being an advocate for this space, especially.

Kate Scarcella 15:57
Thank you. Thank you, Rob. Thank you, Stan.

Stan Wisseman 16:00
Thanks, Kate.

Rob Aragao 16:01
Thanks, Kate. Thanks for listening to the "Reimagining Cyber" podcast. We hope you enjoyed this episode. If you would like to have us cover a specific topic of interest, feel free to reach out to us and you can find out how in the show notes. And don't forget to subscribe. This podcast was brought to you by CyberRes, a MicroFocus line of business, where our mission is to deliver cyber resilience by engaging people, process, and technology to protect, detect and evolve.