Heather (00:03):

Hello, hello. Welcome to the Hurricane Labs Podcast. I'm Heather. And today we're going to be talking about the implications of the water plant breach that happened earlier this month. I have with me today two team members from the Hurricane Labs staff, Roxy and Dusty, and they are going to be talking a little bit more about what happened. Hi, thanks for joining me today.

Roxy (00:35):

Thank you for having us.

Dusty (00:37):

Thanks for having us.

Heather (00:38):

Alright. So Roxy, why don't you go ahead and kick us off with a little bit about what we already know about the breach.

Roxy (00:46):

So this occurred at a water treatment plant in Florida. They had TeamViewer, which is remote viewing software or remote access software should say. So what happened–well, first of all, remote access software is usually is for tech support or for remote employees that are trying to get into a system to work. So I would imagine right now a lot of companies have moved to remote access software during the pandemic. So TeamViewer was compromised by an unauthorized user who tried to put an extreme amount of sodium hydroxide into the water. And there was a plant employee that was watching it happening on the screen who led the unauthorized user complete the action, get far enough to see what they were going to do and then reverted the changes. So the sodium hydroxide was never actually released into the water in that large quantity.

Dusty (01:49):

Also, we found that according to a threat post.com, there was a leaked database of email addresses and passwords on February 2nd that apparently contained 11 pairs of credentials linked to the water plant where the, where the incident happened. So those very easily could have been if they hadn't been updated but since then could have been used to access the TeamViewer account.

Roxy (02:19):

You may have heard my cat in the background. He apparently wanted to give his two cents as well. We said that the computers or the systems in the water plant also had Windows 7 software. So although this was a TeamViewer type of incident when networks aren't updated, it can cause issues like this. So perhaps, perhaps they were running a different version of TeamViewer or something that, that actually hasn't come out in the news. But I'm just saying if they haven't updated Windows 7, they probably haven't updated a whole lot else.

Heather (02:59):

Your cat is very informed on the ongoings of InfoSec.

Roxy (03:03):

Yes. He pays attention a lot. You said mention Windows 7.

Heather (03:11):

So what sort of security issues does this breach bring up then?

Dusty (03:17):

I think first off was the way this past year plus has gone on. We definitely need to be aware of what types of remote access we are allowing into our network with a pandemic and there's a lot more people working remotely. So we need to make sure as security professionals that we can provide safe and easy to use remote access so that our users will be safe when they come out remotely I've often seen how users can take complex tools and find a way to work around them in unsafe ways.

Roxy (04:01):

Right. So also another thing to consider is now that we know about this scenario, let's think about what would happen in our organization. What types of alerts and what types of sensors did they have in place that would have alerted to this.If the plant employee did not see what was going on, if the plant employee was not there to watch the changes being made, I would think, and I would hope that there would be a sensor that would sense an extreme amount of sodium hydroxide. And then there would be some sort of action that would have to take place to undo the damage. So now that we see whenever we hear about new scenarios in the news or from other people, then we have to think, how does that apply in our organization? Are we actually prepared for this?

Dusty (04:55):

I definitely agree with that, and it ties a lot into having layers of defense so that just because someone may be able to get through your firewall, does it mean they have full access to the internal network? Whether the layers of defense are having multi-factor authentication, so if a user's password is breached, they might get a push notification to confirm the login. And if it's not them, they can report it as a malicious login and just having multiple layers of security so that you aren't don't have a single point of failure for your organization.

Roxy (05:35):

And something else that I like to think about is: what if somebody gets the alert? What if this happens? What is the action? Because if people are not informed on how they are supposed to react to alerts, then what's the point of actually having the alert.

Heather (05:51):

Would you say, from what you know about the situation that the plant employee responded appropriately?

Roxy (05:57):

I think so a lot of people think that the plant employees should have prevented it completely from happening. However, I don't know how they could have known what the unauthorized user was going to do. And if there's any action to be taken any sort of legal action, they're going to need proof of what happened. So being able to actually see what the unauthorized user did, not only informed them of what type of scenario was about to happen and are we prepared for it, but it also allows some sort of

legal action to be taken if needed, because if the unauthorized user didn't complete an action, then they wouldn't have any sort of evidence or any sort of, I guess, any sort of way to prosecute.

Heather (06:49):

Now they'd just be guessing at what the person might have been doing. Now, we know exactly what they were trying to do.

Roxy (06:54):

Right. Exactly. And the plant employee knew that they would be able to revert the changes. So nothing actually happened as a result and hopefully they got screen captures as well.

Dusty (07:08):

Yeah, I would, to me, the one thing I didn't like about the whole reaction was the media response to it because it was definitely sensationalized in the media to be this big life-threatening attack that if the plant supervisor or tech wasn't there, it would have caused large amounts of sodium hydroxide to get into the water right away, but reading more into it, I think it would have taken 36 hours for the levels to change. And hopefully they would have had other safeguards in effect to either alert or prevent those extreme changes from happening in the water system. But the media stories surrounding it, made it into a much bigger deal than it needed to be.

Roxy (07:57):

A lot of the cybersecurity industry though functions well with fear, uncertainty and doubt, because that creates revenue. I'm not even sure whose idea it was to report this to the media or why, because nobody was really in danger and it just scares people and makes cybersecurity seem a lot more complicated than it actually is. Incidents like this make people afraid of using technology, for example, and really with any type of technology with TeamViewer, with, you know, your average laptop or server or whatever it is that you're using, there's always going to be ways to mitigate and to respond to threats. There's always something that you can do, whether it's closing a port, updating the software, not using the software, finding different alternatives, finding a different way of doing things, maybe not using a particular feature. I mean, there's always a way. And so when we create fear in the average user, it doesn't really help them at all. We have to be talking about solutions and about what measures were actually in place to protect everyone, instead of just making everyone afraid that their water's going to be poisoned.

Dusty (09:26):

Also fear tends to just make stuff part of the media cycle where, I mean, if you even looking at this, this was a big deal for two or three days. And then nothing since that has been really talked about it publicly. Is this just going to be something that happened and is forgotten about by a lot of people and no changes are made, or can we, or instead of relying on fear, looking at it from an outside perspective and trying to actually implement reasonable changes to prevent it from happening again.

Heather (10:01):

Yeah. I think that's probably the key here is that, you know, just actually learning from the experience and not just for the water plant itself, but other companies, what they can learn from it.

Roxy (10:12):

This does apply to other industries because not only is this a new scenario that perhaps other organizations haven't considered, but whenever something like this isn't the news, it's a good reminder to look at what alerts you have, what types of responses, what the playbook says, and everybody should have a playbook for what they're supposed to do in certain situations, because you have to know, you have to be able to make decisions quickly. And if you don't know what you're supposed to log, or you don't know what actions you're supposed to take, then later on, you may be asked, you know, what was the root cause analysis, or, you know, we're going to prosecute, we need the logs. Oh no, the logs are gone. We didn't collect them. You know, you have to be prepared for every situation and, your team needs to know how to respond.

Heather (11:14):

When you say playbook, are you referring to a vulnerability management policy?

Roxy (11:19):

Well, what I'm referring to is not really a policy, but more of like a collection of procedures and processes that are followed. If this happens, then do this.

Heather (11:32):

Gotcha.

Dusty (11:32):

I also highly recommend actually doing tabletop exercises with your playbooks. So that the first time you are thinking about how you would actually respond in the situation, isn't in the middle of a high intensity, high emotion breach. So you know, who need to contact, what you need to, like Roxy said, what you need to collect and actually have practice going through those steps. So you can find the parts that may be don't work as you expect them to, or take more time than you would expect them to and how that stuff written down and known about in advance.

Roxy (12:16):

Oh, and also make sure that you're logging and alerting on your assets as well, make sure that you know your assets, make sure that you know who has access to them and that you're revealing access and you have a procedure for revoking access whenever somebody needs the company. Also, a lot of industries like the banking industry, for example, are always looking for credential leaks and credit card number leaks and PII leaks. They will search the internet and search the dark web and make sure that the sensitive data is not out there. So I'm not sure how they found the leaked credentials, but it is possible to find those credentials on forums and on, you know, paste type websites like Pastebin, or even through monitoring IRC or monitoring, now IRC is less commonly used, so monitoring discord channels. So there are ways to look for sensitive information and financial, the financial industry is really good at this. So if you know someone in the financial industry, they might have more information on it, but other industries could do that as well.

Heather (13:45):

Alright. Well, thank you very much for joining me today.

Roxy (13:49):

Well, thank you for having us.

Dusty (13:51):

Thank you for having us.

Heather (13:51):

For sure. And that's all for today, folks. Thanks for joining us and be sure to check out our resources for more information. Until next time, stay safe.