PWNED Transcripts – Season 2 – Episode 2 – Securing Your Remote Workforce

This is Pwned, the weekly podcast for cybersecurity professionals. We answer your cybersecurity questions and share stories from the trenches about how security professionals, security engineers in CSOs are protecting their organizations. Today we are talking about how to secure your remote workforce and whether your workforce is already remote or newly remote as a result of the recent pandemic. We'll be going through some tips for organizations on how to secure your workforce. Pwned as always is brought to you by a NuHarbor Security, your end to end provider of security services and security solutions. If you're looking for complete cyber security protection for your business and a security partner, that actually gives a BEEP , visit us at www.nuharborsecurity.com.

Now, when we start to think about securing a workforce, there's generally two scenarios that we want to think about or how we kind of approached this situation. The first scenario is that you're forced to secure your workforce on a short notice, kind of an emergency situation. You're doing what you can to make things work. Doing the best you can given the circumstances. The second scenario, whereas if you find yourself in the fortunate position where you're able to plan in a medium or long-term situation on how you would strategically secure your remote workforce and you have the luxury to plan, that's additional considerations to take. If you are in a pinch, there's things that you can do from an it administration standpoint and there's things that you can do from a user standpoint. The best thing that you can do is to spend your time educating your workforce on phishing and associated cyber scams. So when we think about phishing, we think about phishing attacks. Today, the statistic is 92% of security incidents occur through phishing activities. Given the nature of covert emails or Coronavirus emails, that is all seemingly relevant news and interesting

topics that peak your users curiosity. People that are phishing and trying to use that avenue of attack into the user base are disguising nefarious emails in the form of the Coronavirus or COVID type news or alerts and order to spoof scam your user base.

So when we think about trying to protect the workforce and what's the biggest bang for the buck and where should the most time be spent? Some simple education and some careful consideration to inspect emails before opening or engaging in any links within the emails could get you a pretty high return on investment. If you are an IT administrator, tactically there's some additional things that you can be doing to secure your organization. If you don't have one already, you can implement an email security gateway. What this gateway would effectively do is filter and block any nefarious or maliciously crafted emails looking to scam your employees. Some examples of gateways could either be, Proofpoint or a Mimecast type solution that could help you filter out some of those nefarious emails. The second thing that you can tactically do is implement strong endpoint protections for your corporate devices.

When we think about the endpoint security space over the last couple of years, that vertical within cybersecurity has come an incredibly long way. The industry has made a fundamental shift away from the traditional antivirus to the true next gen antivirus as well as EDR solutions, which gives organizations the ability to track, monitor and remotely quarantine infected machines. So the example being, with one of these solutions in a remote workforce, not only can you track which machines are infected at any given time, you can also proxy the web connection effectively. Taking that machine offline remotely, stemming any potential cyber attack that might be occurring at that time. And lastly, if you're really concerned, how do users change their passwords in an over abundance of caution? Within our organizations too often we see widespread account password compromise. So your users might have had their email addresses and passwords

compromised by a third party site that has subsequently published out to the web.

Those credentials might be a foothold into your corporate environment. If that is a concern for your organization and you're worried about it, taking those cautious steps, forcing your users to reset a password that is complex in nature, and different from what was previously configured might stem off some potential cyber attacks that could be occurring. Now, if you are a user looking to operate in a newly remote work environment or you're looking to secure an already existing remote work environment, there's four media things you can do to secure your work environment. The first one is to avoid public Wi-Fi at all costs. So staying off public Wi-Fi or wi-fi's that are being shared with other users could be the first step. It is well known that shared Wi-Fi can introduce a security weaknesses with how you transact and connect within your organization. Depending on your internet connection, your data could actually be snooped over the wire by someone who's sharing that same Wi-Fi connection.

So the first one is to stay off public Wi-Fi. Focus on using home Wi-Fi or personal hotspots that you know, you're the sole user of. The second guideline is to keep work on work computers. Meaning if you have the luxury, do your work on your work computer. If you have personal stuff to do, do it on your personal computer. Too often we see that folks being forced to work remotely under short circumstances end up co-mingling those two things. And sometimes even see that kids get access to work computers, which introduces some security issues. So second recommendation is keep work on work, computers, personal stuff on your personal computers. The third recommendation is to physically block sight lines to your computers. So too often that we see users working on work documents, either at you know, public location, an airplane or generally as a shared work environment. Being able to keep someone from doing a shoulder surf and looking at your screen can help secure information that you're currently working on.

And then lastly, the fourth recommendation is always look to encrypt sensitive data. So if you are in doubt, you can never be faulted for encrypting or using encryption if you're unsure. So by always taking it a default of always encrypting data, you can be sure that information will always be protected. Now if you find yourself in the fortunate position of having time to plan. So you are planning for a remote workforce in the medium term or potentially long-term, there's things that you should start thinking about and there's things that you can do to secure your remote workforce. And five things to think about, first one is your cyber hygiene is important for your organization. So having strong patching programs and having hardened system configurations can help you ensure a strong cybersecurity hygiene for your environment. In order to do some of these things requires that you have the foresight and the systems to be able to do remote patching and remote system hardening and configurations for your workforce.

The second item is having a level of visibility to remote workforce is also important. This is also significant because the cybersecurity industry is now at a point where the technology allows for the level of visibility that you would need within your organization to track and alert on devices that are not necessarily connected to your corporate network but might be a corporately owned device. The third recommendation is to leverage cloud technologies and cloud architectures as much as possible. The truth of the matter is the cloud landscape today and large cloud providers have invested in the security technology required in order to secure their own stack. For examples, take AWS or Microsoft O 365 or Google docs. Some of these larger organizations have invested in security technology and they've invested in the security horsepower in order to secure their stack. If you include some of these large scale and scalable cloud offerings within your cloud architecture, it could be a way to extend your security footprint and your security reach and securing your remote workforce.

The fourth one for larger organization and larger corporations, incident response plans must be adaptable to being executed by a remote workforce. On the NuHarbor side, too often we see incident response plans that have a heavy reliance on having the team work physically together and being in the same physical proximity in order to execute and deliver on that plan. But when your workforce is remote, you're distributed, you're responding to an incident where everybody's remote can provide for some interesting complications and communication challenges. So, in the medium, and long term, when you start thinking about designing your incident response plan, having those remote contingencies in mind will make your plan a little bit more scalable, and ability to be executed in emergency situations. The last one, and probably the least sexy of all of these is develop strong security policies. So having those pre-thought through and premeditated written security policies to guide staff on what's permissible or what's not, can give your staff the guidelines that they need in order to self select the correct security decisions when they have no one else to answer some of their immediate questions.

And then from a tactical standpoint, technical policies such as Windows system policies to protect your staff should also be implemented because accidents do happen. And having strong Windows systems policies or Linux systems policies can help prevent some of those incidents that might actually lead to an accidental cyber breach. So those were some tips and techniques that you can use to secure your remote workforce. As always, thank you to NuHarbor Security for sponsoring this episode. If you are looking for a trusted security partner that actually gives a BEEP, please visit us www.nuharborsecurity.com. In next week's episode, we're going to be talking about security, orchestration and automation for MSSPs.