You're listening to the one HCL podcast series, the place where industry experts, analyst and veterans help us identify, understand and prepare for the upcoming cybersecurity technologies and trends. If you haven't subscribed to the channel already, do it now for regular updates. This episode starts in 321.

Hi, everyone. Welcome to the cybersecurity and GRC services technical podcast on vulnerability management. I'm your host for today. And with me today I have Saurabh Singh, who is leading sales service security consulting team and has extensive experience in various cybersecurity technologies and offering so Saurabh has an extensive experience of around a decade and vulnerability management domain, which is a topic of discussion for the podcast. So let's start our today's podcast and gain some in depth industry information in the field of vulnerability management from our guest, welcome to our podcast Saurabh
Thank you. Happy to be part of your podcast
today. Thank you, Saurabh. So, as a kickstart sort of can you give us an overview what vulnerability management is all about?
Sure myth. So, vulnerability management, as a word as a security control has gone through a sea of changes in its definition and usage over decades. Earlier, it used to be only an additional security responsibility, but now it has become a cornerstone of any successful security programme. There is a difference between vulnerability assessment and management. But if we talk specifically on definition of what vulnerability management is to bring it in a nutshell, vulnerability scanning can be defined as capability which is achievable by a security application that is can enterprise networks identify weaknesses and vulnerabilities, vulnerabilities which can include different products misconfigurations on the operating system side or if we broaden the definition, it will end income pass misconfigurations on hardware and software side software services which can act as common points and shortcomings which can be targeted by any ill-intentioned hacker or user. So, on a high level, this is the definition for vulnerability assessment and management.
Okay, so we can understand your answer that vulnerability assessment is innovative relative to the validity management programme. So sort of can you just throw more light on this that how vulnerability assessment and management are interrelated with each other?
Definitely.
So vulnerability assessment and management as the name suggests, vulnerability assessment is one phase of vulnerability management cycle will MBT assessment is the phase wherein we perform the scanning get a view on the security posture of my assets, whereas vulnerability management then takes on this output from vulnerability scanning and focuses on doing prioritisation and closure of the vulnerabilities which are reported on an ongoing fashion not as a one-time task. So, that is vulnerability management.
Okay. So, sort of you talked about the vulnerability assessment being a part of anti-management cycle. So, can you just also let us know what are the components of a typical vulnerability management programme?
Sure. So, if we talk about vulnerability management programme, there are two aspects of it to understand from it. So, one is the, so, I mentioned it vulnerability management tool as the security application. So, what are the components of this application? And second aspect would be what are the aspects or components of a vulnerability management programme. So, to answer the first part of the brain of any vulnerability management tool is the scanning capability. So, which is achieved by competence called scanners, the hardware or software devices which can be deployed in any network to scan the network get visibility

on vulnerabilities. Now, there has been upgrade on that front as well wherein not only scanners but we also see scanning agents, passive network scanning agents, so, multiple types of options are available to us to perform with limited scan. Coming back to the second point of your question, which was what are the components of vulnerability management programme or what are the phases It is a very clear multi step process. Starting with discovery where then we get a visibility on the asset landscape of our organisation Then building on that visibility, we perform scanning, getting the viewpoint on what are the vulnerabilities or the weaknesses which might exist on the assets operating systems or the applications for that matter. From here, then we go towards remediation, whether they ported vulnerabilities have been remediated or not. And then once if it is remediated, how do we bring up confirmation? So, this is the face of a vulnerability management programme. The vulnerability management programme that we just discussed has been referenced in various industry best practices and guidelines. Okay.

Thanks for the detailed explanation on the vulnerability management and now I believe all our listeners should have a clear picture of what actually a vulnerability programme is. So, Sora as you just talked in the last part of your answer that you have some industry basics best practices. So, can you let our audience know what are the industry based best practices which are utilised in the world in a typical vulnerability management programme?

Definitely a myth. So if we talk about the best practices, so what I'll say is, there are multiple government regulations or industry standards, which mandate or which explicitly asked for the performance of a regular vulnerability management programme. So, to name a few there are PCI DSS HIPAA FISMA standards like ISO 27,001 or the one which is explicitly asked or mandate the use of vulnerability management programme. However, there are other definitions in in standards and regulations as well which might not be explicit, but the compliance officers and alters the interpretation which they get from the other standards also mandates that there has to be a well defined vulnerability management programme which is followed rigorously throughout the environment.

Okay, so, sort of these standards differ from industry wide list based on industry, whether it's a manufacturing or financial industry. So, are there some standards applicable to a specific type of industry

definitely among the examples that we gave for example, if we we talked about PCI DSS PCI DSS stands for payment card industry data security standards standard which is specifically followed by organisations which are dealing with credit card data hence it is more relevant to organisations which deal with credit card data and the other one for example, HIPAA are more applicable to organisations which are dealing with medical data. So those are the regulations and how they differ for the vulnerability management requirements as such.

So, basically we can make out that this is a dynamic revenue management programme based on the industry wide best practices, sort of usually we hear a term named as penetration testing interchangeably with our management. So can you throw us some light over what basic penetration testing programme is and how it differs from vulnerability management?

Oh very well, important comment. So see, when we talk about standards and regulations, what they talk about in this same breath is vulnerability scanning, penetration testing 20 years monitoring of compliances and then the other vulnerability management practices. Now while the penetration testing and vulnerability management is being talked about in the same breath, but there is a difference in the definition of good the services if we talk about vulnerabilities in a very basic language, it is a tool based weaknesses on network assets, server assets, and the third party applications which might be sitting on top of it whereas penetration testing goes a step ahead and it involves manual exploitation of the vulnerabilities which have been reported by the tool and once the vulnerability scanning completes, then the penetration testing begins power by requirement both are different and the frequencies and the complexities involved in both the service areas are different. Okay. So, we can think like this that once the vulnerability assessment has been completed and the vulnerability report is there, then based on the service, either PT can be performed or we can go with vulnerability management emulation programme. Exactly. Um,

so if the requirement is for penetration testing, definitely we can use the report which is there with us, either on the infrastructure side or the application side.

Okay, so sort of, I believe this was a bit technical stuff, and I think all of our audience who is also from the cyber security domain will be very much interested in knowing in detail what the penetration testing is. So sort of moving ahead, we are continuously seeing that threat landscape increasing over year by year basis. So, how do you relate these different threat vectors with inefficient vulnerability management in the organization's So,

I mean if you will see the trend, so, if we say that the data breaches are increasing or the advanced persistent threats are increasing, what is the target that we are to see? So, the targets which the hackers have in mind is to take advantage of that we can gain access either to the organisation or organisational critical data. Hence, what the focus on is, if there are vulnerabilities which exist on desktop side applications, operating systems, plugins and servers. So, those are the common avenues which are targeted. Hence, it becomes imperative for organisations that this the vulnerabilities which might exist is identified and removed in a timely fashion, as per the criticality of the vulnerability for our organisations. Sort of your answer clearly depicts that how well HCl is evolving itself with the ever changing client requirements. So, now, I think with this podcast, our audience had got an overview about the vulnerability management and the advancement of multi management, which is just taking up the industry standards and the various industry solution offerings and our latest client requirements, which is sales volume demand team is going through. So well that's for today's episode of sales consulting and I sell cybersecurity and GRC services podcast. Thanks for listening. And thank you so much for joining me today for sharing your valuable experience on the most important pillars of the cyber security domain. That is the vulnerability management. Join us again when we will talking about the penetration testing, which is also another important cybersecurity pillar to thank you everyone.

Good man.

This episode of the one HCl podcast series has ended, but be sure to subscribe for more insights on how to identify, understand and prepare for the world of possibilities around the new and upcoming cybersecurity technologies and trends. Don't forget to rate and review the episode so that we can keep bringing you the most relevant content. Thank you for listening