Cyber Safe Cities Podcast

Security Audits and Assessments with Kevin De Snayer, National Cybersecurity Strategist with Calian Inc.

[00:00:00] **Tenielle Bogdan:** Welcome to the Cyber Safe Cities Podcast. This podcast is brought to you by the Municipal Cybersecurity Best Practices Initiative led by TECHNATION Canada and funded in part by Public Safety Canada under its cybersecurity cooperation program. This podcast looks at the ways Canadian municipalities can ensure they are cyber safe. To learn more, head to technationcanada.com and check out our Municipal Cybersecurity Best Practices Guidelines

Thanks for tuning in. I'm your host, Tenielle Bogdan, and today we are chatting with Kevin De Snayer, National Cybersecurity Strategist with Calian.

Calian is a world renowned company with offices and projects that span Canada, the United States and international markets. Kevin has spent the last two decades leading a team of security experts that are sought after by government, academia and commercial organizations to provide end-to-end cybersecurity solutions.

Kevin has spent time on both the national rugby league and Olympic luge team. He brings that same passion and ability to push the boundaries of failure to the world of cybersecurity. Today, we are chatting with Kevin about security audits and assessments.

Hi Kevin! Thanks for chatting with us today.

Kevin De Snayer: I'm excited. And thank you for doing this. It's important that we work together to get these cities a little more secure.

Tenielle Bogdan: Tell us a little bit about your work with Calian and how that applies to municipalities across Canada.

Kevin De Snayer: I have an interesting role. I'm the director of our cyber services division and our also our National Cybersecurity Strategist. In cybersecurity, one of the interesting thing is a lot of organizations want to hear what other people have to say, but they don't want to give up information on what they are doing.

In my role I get exposed to a lot of different municipalities, federal government, provincial governments, and commercial industry. As Calian is a global company, I'm also getting to see different industries around the world.

Tenielle Bogdan: Today we're talking specifically about security audits and assessments, which are becoming increasingly more in demand as our world becomes more interconnected and globalized.

Can you chat about the importance of these types of audits and assessments to municipalities and how they can get involved?

Kevin De Snayer: So step one is to identify your path – your cybersecurity path. You need to know where you are at and where you need to get to.

Security audits and assessments can start very, very basic, but the first thing we need to identify is the main purpose and where we are at today, so we can help find and expose gaps that you may have.

We’ve done these as basic as an audit. So here's a checklist: Do you have a security procedure in place? Are you documenting any progression? Are you doing any kind of education with your staff members? Do you have key performance indicators? Do we know where we are now, and where we would like to be?

A lot of times we see organizations that have a security posture in place where they have a firewall, security software running on a machine and that is it. There’s no real gain on increase in that security posture with these organizations. But this is a great place to start assessing where the gaps may be.

Once identified, then we can talk a little bit more detailed as we move forward into the actual vulnerability assessments (VAs) and the penetration tests.

With municipalities, we really need to work on the threat intelligence that our organizations see and how to chare that information to prevent future attacks.

Municipalities see information from policing, to ambulatory, to people's paychecks, which many people need access to. With all of these users, its much more difficult to secure the information and lock everything down.

The another part of this information sharing between municipalities could be is security forums. Calian has done some of these in the past where we bring a bunch of users together and we throw them in a room and have them talk about what they're doing now. We need to continue doing this and bringing the right groups together to talk about cybersecurity and information sharing.

Tenielle Bogdan: Absolutely, partnerships are key. It's a common thread that we're seeing across all of our podcasts. sYou touched a little on a VA tests and pen tests. Can you chat a little bit about the differences between those two and

Kevin De Snayer: This is when we're actually starting to put the pen to paper and to start to figure out what we need to do, based on what we already know.

The lines are coming a little bit more blurred between a VA and a pen test. Anecdotally, a VA test is where we sit across the street with binoculars, and see what we can find inside. We start to evaluate the weaknesses in the house – is there a window open? Is the door a little older where you can pick a lock? Is there a tree outside that we can climb to gain access inside?

Now, VA’s and pen tests are coming closer together and can be done as one exercise. One of the big changes you have is red team testing and blue team testing, where your red team acts as the attackers and the blue team is the defending side.

There's just different techniques and strategies that you need to defend against the problem with this old red team and blue team pen test. We're all competitive in the world that it's human nature and the way it was set up. It's us against them and them against us, with no collaboration. A lot of the time, the red team would do on, run their tests without the blue team or the corporations knowledge, and report back without any collaboration from how the blue team would respond. With that, now we're starting to do what we call purple testing.

This is now where you take somebody from the red team and the blue team, and you sit them down at a table, with management and other key team players to find solutions to the gaps in the systems.

For example, maybe as an organization, you say, “yeah, we've got a firewall in place. We think we've locked down and people are getting remote access. We’ve updated a couple policies.” The red team could sit back and explain how they are going to run the attack, provide live data and a live threat stream, in an effort to work together on what the problem looks like and how to come to a solution.

They can evaluate a real time response. Did the team reply back? If not, why didn't they reply back? And now you're getting immediate feedback and making changes in real time.

Tenielle Bogdan: What are some things that municipalities should identify before proceeding with a security audit?

Kevin De Snayer: Having a strong understanding of the scope of work that you're trying to do.

Cyber security is again, it's an ever-changing field. It grows on a daily basis. There's something new every day with what you're working on, you can't fix it all at once.

There's just so many different areas, but again, we're all here because there's a risk and we need to mitigate some of that risk. When we sit down with the client, we will ask what are the risks that you're most worried about? What have you put in place already? Have you done any internal table team tabletop exercises? Do you have a working group engaged? We need to collect all of that information to get a very clear scope.

The nice thing to see is cyber has now become part of vaster business risk management, where it was previously managed separately.

Once we have a starting point, we can start moving towards solving some of those problems that those users have and take it to the next step. And then we can take it to the next step.

So a very, very clear scope is the first step, and then a clear understanding of what risks you believe you have inside of your municipality is the second.

Tenielle Bogdan: What are some common risks that you see with municipalities?

Kevin De Snayer: The biggest risk that municipalities have is that they are carrying a lot of personal data. They have an abundance of information that many people need access to.

We also see one of the challenges in municipalities is as a citizen, we have the right to communicate with our elected officials, but that obviously causes a challenge, as there is spyware, there's phishing attacks, and there's social engineering attacks that are happening on these organizations, while citizens still need access to their elected officials. As a commercial organization, you can block people and put in safeguards to prevent phishing and social engineering attacks. With municipalities, it’s not that simple as they may not be blocking or preventing one of their citizens access to the organization.

The other challenge is clear policies because again, cybersecurity moves very fast, which does not necessarily correspond with the pace of the business of municipalities.

Right now, we're looking at 70 plus percent of all internet traffic is encrypted using something called TLS. We see this at all levels of government and commercial business which may not have the right to decrypt users, traffic coming in or out of their network because the policy is older than when this technology was available. And this where most of the threats and malware is coming through. That's where a lot of people can exfiltrate data out of your organization if you can't decrypt SSL traffic, cause your policy says that that's not allowed at this point or you don't have the technology in place to do it.

Tenielle Bogdan: Is there any tools or, or things that you can touch on or provide, that municipalities can do to secure that data?

Kevin De Snayer: That's a fantastic question, and a very challenging one, especially as we get to the world where almost every organization is hybrid. Employees have access to organizational information in their pocket through cellphones. I can’t even imagine what types of confidential documents are being printed at home printers and not being shredded or disposed of properly.I’m sure we could do a whole, another webcast on the challenge of that data.

What we’ve learned over the past two years is that the technology wasn't kept up with in industry. There wasn’t a proper investment in IT services and the security around it. Sure, you may have a firewall, but is the policy around that firewall out of date? Maybe it’s time to look at a next gen firewall where you have the ability to SSL decryption and have end user behavior analytics.

This technology identifies the fact that somebody logs in every day around eight o'clock in the morning and they only log off at four o'clock as something that’s pretty regular. The odd time, they may log a little bit outside of that. All of a sudden now at three in the morning, they log into a device where they did a password wrong four times, and then they downloaded a whole bunch of information. End user behaviour analytics flag this and allow you to see that something is out of the ordinary.

We also see a lot of organizations, especially in municipalities running traditional signature based security, where you have a list of people or email addresses that are blocked from your system. In the case that there is someone that is not on the list because we have not seen them before, we may let them in for a lack of knowing how “bad” of a player they are. With EDR or XDR detection we can start to eliminate these other potential risks..

And lastly, the biggest challenge is as talent. One of the difficult parts of being in cybersecurity is that it changes so fast. So to be successful in cybersecurity, you have to be a person that naturally wants to continually research, continually be reading, and continually update your skillset. Municipalities face this in a lack of dedicated cybersecurity talent and how that corresponds with budget considerations.

Tenielle Bogdan: We know that resources are spread thin for municipalities and unfortunately cybersecurity is sometimes an afterthought. So by starting somewhere, we're hoping that the work that we're doing will be able to help secure some of these organizations and, and provide just kind of base level awareness of the things that they'll need.

And hence why the Municipal Cybersecurity Best Practices Guidelines are live on the TECHNATION Canada website. It's a great starting point for municipalities to have a peek at, to look at and just to be aware.

Kevin De Snayer: Yeah. And it helps a little bit even getting the culture changed inside an organization. A lot of times where we saw original cybersecurity, even cyber awareness training is so important to users, but it was a penalty almost. you accidentally click on a real live phishing email, people are afraid to talk about it because they're worried about getting fired. So the culture needs to change in that your have to work together with IT and the cybersecurity teams.

There's actually people that will correct your literature for you, so you can create a spam or a phishing attack, send it to somebody, they would pay them on the dark web and they will correct the literature, and correct the language on it and make sure that it's written correct. Send it back to you, you pay them the funds.

And now these, so these attacks are getting much more accurate to end targeted to the users. We really need to establish that culture, and upper management needs to be part of it.

People are not hacking into networks as much anymore. They're stealing your credentials and just logging in. So two factor authentication is a big way to mitigate that.

Tenielle Bogdan: Yeah. It’s all about demystifying, cyber security.

Kevin De Snayer: Yeah. And, and we're getting better at a lot of it.

Like the education is a tough part and in our own organization at Calian, we're going through this and its changing the narrative from “oh they’re making me memorize a lot of terms and this training takes a long time” to “ this is going to make be more aware of how I can secure my organization”.

We think about it, but don't be afraid to tell somebody if you think you've done something that you shouldn’t have.

Tenielle Bogdan: You’ve provided a lot of wonderful pieces of advice and information for municipalities today. But if you can provide our listeners one tactical piece of advice or tool or technique to take away, what would that be?

Kevin De Snayer: Don’t underestimate the “bad guys”. The adversaries, like they, the, the bag, the bad actors, bad guys, hackers, pen, whatever you want to call them, they are getting smarter. They're state sponsored. Their funding is higher than most of us are running their cybersecurity programs under.

So don't underestimate them, and even more importantly, be aware of your own vulnerabilities and weaknesses. Really understand where you are at in your cyber journey, and make sure you're aware as much as you can about what's out there. That comes from communicating across different organizations, different municipalities, and trying to share as much information as we can with each other.

Tenielle Bogdan: Thank you very much to Kevin and his team at Calian Inc.. To get connected with them, head to their website https://www.calian.com/solutions/cyber-security-solutions/.