MPR News | Minnesota Now Expert: Minnesota water systems need updating to prevent future attacks 01KZ4DF3B53119JZXSSSBT1S7F

KELLY GORDON: This is *Minnesota Now.* I'm Kelly Gordon, in for Nina Moini. Minnesota's water systems were attacked last week, and we weren't alone. Seven states were targeted in all. That's according to new reporting done by *The New York Times* over the weekend. *The Times* also reports that federal officials suspect Iran may be behind the attacks, although that investigation is still ongoing.

Plymouth, just northeast-- or northwest, excuse me, of downtown Minneapolis, was one of the cities that dealt with the cyberattack. Public Works Director Michael Thompson says it wasn't their drinking systems that went down, but the sanitary systems and two water towers.

MICHAEL THOMPSON: So the 14 lift stations that we had go offline temporarily, those actually pump sanitary sewer water into the pipes that go into St. Paul ultimately to get treated. The only water infrastructure that was related here was just the PLCs and the two water towers. So we just couldn't take real-time readings of pressure and levels. And so that's where we had to send physical staff out there to take pressure readings to make sure we were monitoring the real-time condition of those water towers.

KELLY GORDON: And we're going to learn more about those PLC controllers in a moment. Thompson also shared with *MPR News* that since last week's attack, there have been more attempts to hack into Plymouth's water systems.

MICHAEL THOMPSON: Once the cyber hack was isolated, we worked with our partners to properly mitigate the risk. And we believe we've addressed that. Even though there's been attempted intrusions since, those have all been blocked. But we continue to monitor. But for any incident like this, there will be lessons learned. We want to learn lessons. If there's things we can share with others, that's ultimately what we want to do. We want to make sure we're protecting the infrastructure. And as unfortunate as these incidents are, if there's things to be learned, we want to take things away from that.

KELLY GORDON: That was Plymouth Public Works Director Michael Thompson. We're going to turn now to a cybersecurity expert. Faisal Kaleem is a cybersecurity expert with Metro State University. Welcome back to the program.

FAISAL KALEEM: Thank you very much, Kelly.

KELLY GORDON: Yes. So let's start here. US Senator Amy Klobuchar says the hackers targeted specific brands of control systems that are used by water utilities in Minnesota. Can you explain what makes these systems vulnerable? I know that in Plymouth, that public works director there, he called them PLCs.

FAISAL KALEEM: Yeah, thank you very much for the question. So just for the listeners, let's put some technical terms, first of all. So PLC stands for Programmable Logic Controller. Think of these as rugged industrial computers that executes instructions, such as when to start a well pump or open a valve. So some of the related terminology you may also hear in these kind of events, like for example, HMI, that stands for Human Machine Interface. This is a screen that operators use to view levels, alarms, and equipment status, and issue commands.

Now, obviously, if these PLCs and if these HMIs get compromised for any reasons, the attackers are able to modify the readings, modify what the operator sees, and then they can do some severe damage. The reason why these PLCs are vulnerable, because they are not easy to replace. And they cannot be updated because they are using some sort of legacy systems. And then they cannot use some sort of modern authentication systems or authorization systems.

KELLY GORDON: So it's safe to say they're pretty old in terms of computers and things. They work, but they're vulnerable because they're just antiquated.

FAISAL KALEEM: Yeah, antiquated. And one of the other reasons why they become so vulnerable, because as soon as these PLCs or these HMIs related systems are connected to the internet or any sort of cellular communication mechanism, which the hackers can access, now all of a sudden, if there are any vulnerabilities that are present inside these computers or rugged systems, now these vulnerabilities can be exploited by the attackers.

KELLY GORDON: Right. Michael Thompson, the Public Works director in Plymouth that we heard from, he mentioned that there have been more attempted attacks since. Do you think it's likely the same attacker? Or is this maybe even new attackers who saw that vulnerability and are wanting to exploit it?

FAISAL KALEEM: Yeah, so here was the issue. What I believe is that the vulnerability that was exploited, there was no patch available. Patch simply means that there was no update to the vulnerability or the vulnerability was not fixed in time. So what happened was that once the vulnerability got exposed to the world wide web, then it becomes known to every attackers, not just the nation-sponsored attackers. So it could be nation-sponsored attackers, or it could be some these script kiddies or people who are basically looking for just taking systems offline or maybe demanding for ransomware.

KELLY GORDON: Right. What do you make of the reports that Iran may be behind these attacks, initially, the first wave?

FAISAL KALEEM: So just to be clear that, yes, the public assessment says that Iran or Iranian-backed militia might be, I mean, they are using the term "Cyber Avengers," that's the name of the group, might be behind the attack. But US officials yet to have made that attribution. So they have not yet officially attributed to Iran.

So what I would say is that it could be Iran, it could be Russia, it could be China. There could be any of these adversaries who are basically after US interests. So, I mean, again, it doesn't surprise me that if the US comes out and say, hey, that Iran basically was after this attack, and especially in the wake of the political stuff that is happening right now.

KELLY GORDON: Right. In Plymouth, it was sewage, as we heard, not their drinking water that was impacted. But still, water systems, when we hear about this, it's critical infrastructure. My colleague, Emily Bright, said in a meeting this morning, infrastructure is super boring until it goes down, and then it's really important. So what are the risks of systems like this that we don't necessarily think about every day, but that impact our daily lives, of these systems being attacked in the future?

FAISAL KALEEM: I mean, again, the same thing. Any systems that are vulnerable will be attacked, OK? So the responsibility falls onto us, which means that we need to make sure that we need to keep an eye on these vulnerabilities. As soon as these vulnerabilities come online or become available, we need to make sure that they are properly patched or taken care of. So, again, I'm not going to be surprised if we are going to see these kind of attacks in the near future because our critical infrastructure sector is vulnerable.

KELLY GORDON: Right. Do you know what steps might be taken right now by some of these infrastructure systems to prevent this? Because I have to imagine that what you're talking about, updating them, this is expensive.

FAISAL KALEEM: Yes. So obviously, what they did, I'm going to really commend them, that when they moved to the manual operation, that was something, what we call resiliency. But the most important thing is that when it comes to these industrial control systems, they need to be segmented. We need to make sure that there is no unnecessary internet connection to these vulnerable systems.

And then the other important thing is that we need to invest in cyber hygiene. Cyber hygiene is basic cyber hygiene, which is basically like, hey, not to use the default credentials, not to fall for these phishing emails and all those kind of different things. So unfortunately, we don't do a good job to provide those cyber hygiene to our municipal workers and leaders.

And thirdly, what we need to do, we need to also invest into continuous monitoring. So I am happy to say that Metro State, here at Metro State, we actually have implemented a student-led security operation center that we would like the counties and cities to take advantage of. The student can be trained to become the next cyber defenders while they provide free community services monitoring these underserved municipalities.

KELLY GORDON: That is really fascinating. That is definitely something I saw this weekend, is that we're asking these small cities, municipalities, to take on this really big threat because of the vulnerabilities that they have that is really specific. So that's a great idea to pair these students with these municipalities and try to do some protection. I'm curious what you'll be watching for as this situation goes forward.

FAISAL KALEEM: Obviously, one thing that I'm going to be watching for is to see if the US officials comes out and say that, hey, this is really attributed to the nation-sponsored attackers that the public reporting has been suggesting. But on top of that, I definitely will be looking out for-- I mean, I hope it's not going to happen, but we know, as you mentioned, that there are seven states, two states publicly announced, Michigan and Minnesota, 45 municipalities. I hope this should not continue. But if it continues, it's not going to surprise me.

KELLY GORDON: Yeah. Have you heard about any other attacks at other places, other states or cities that they didn't actually get through, but they saw that there were people coming up against it?

FAISAL KALEEM: No, the only thing that I know from the reporting is 45 municipalities across seven states. And two states, Michigan and Minnesota, they are the ones that publicly said that, yes, their municipalities were attacked.

KELLY GORDON: Right, OK. Well, I really appreciate your expert today, Faisal. Thank you for joining us.

FAISAL KALEEM: Thank you very much, Kelly. Take care. Bye.

KELLY GORDON: Faisal Kaleem is a cybersecurity expert at Metro State University.