NSA and CISA Call for "Immediate Action"

The U.S NSA (National Security Agency) and CISA (Cybersecurity & Infrastructure Security Agency) recently issued a joint alert1 where they urge "Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems".

The background for this alert are the recently reported2 Iranian cyber-attacks against Israeli infrastructure3 where "cyber actors have demonstrated their continued willingness to conduct malicious cyber activity against Critical Infrastructure (CI) by exploiting Internet-accessible Operational Technology (OT) assets".

It was reported that the Iranian hackers' apparent goal was to raise the level of chlorine in the water supply by changing the logic of the PLC without raising any alarms. Hundreds of people would have been at risk of getting sick had the attack succeeded. As SIGA demonstrated in the past, US officials are now officially stating that the Israeli cyber-attacks have and may also in the future cause a grave impact on critical infrastructure. A joint alert by the NSA and CISA are not very common, which makes it obvious that US Authorities are now no less concerned that a similar attack may happen on US soil, thus raising awareness to increase their cyber resilience, using a list of recommendations.

But the question that still remains is how well can these measures be used in order to tighten and mitigate the exposure for these kinds of attacks?

Out-of-Band Monitoring

malicious cyber-attack on operational machinery and equipment". Implementing the SigaGuard solution, can effectively detect and mitigate any OT related attacks, regardless of the attack vector used by the hackers and regardless of their sophistication.

https://us-cert.cisa.gov/ncas/alerts/aa20-205a

https://www.ft.com/content/3ea57426-40e2-42da-9e2c-97b0e39dd967

https://www.cyberscoop.com/israel-cyberattacks-water-iran-yigal-unna/

https://sigasec.com/wp-content/uploads/2020/07/SIGA-cyber-campaign-04.06.2020-1.pdf .

Learn from the Israelis

Furthermore, the Israeli regulator itself, the Israeli National Cyber Directorate (the INCD), has included level 0 monitoring in their professional document called "Reducing Cyber Risks for Industrial Control Systems (ICS)"5. In their own words they recommend (p. 57): "measuring changes from sensors and actuators (level 0) in a completely disconnected configuration of the operating network (out of band)". This recognition relays the fact that level 0 is the most critical layer to monitor and can provide an independent validation of the real-time status of the process and equipment. In simple words, there is no real other way to make sure that OT processes indeed operate as intended.

What can we do Today?

Should we be concerned? Yes. Should we panic? No. There are many gaps in OT cybersecurity waiting to be bridged. Building a wide range cyber resilience plan is important, but there are simple measures that can be implemented today, without any delays.

Siga offers critical infrastructure operators greater operational reliability and control over mission-critical systems – preventing service interruptions and enabling full compliance with strict regulatory regimes including the "US Water Infrastructure Act of 2018" and others. With Siga, operators can be confident that they know, anywhere and in real-time the exact status of every critical component.

The good news is that SIGA is here to help you take immediate steps towards a safer operating environment.

https://www.gov.il/BlobFolder/generalpage/icssolutions/en/ICS_eng.pdf