OT Security

Cyber-Physical Systems are all around us today. Operational Technology (OT), a subset of the concept of Cyber-Physical Systems, has been used for decades in asset intensive industries like Oil & Gas and Manufacturing. It also plays a key role in Critical National Infrastructure like energy, water, transport and dams. The rise of consumer based Cyber-Physical Systems like smart thermostats and autonomous vehicles led to a ubiquitous Cyber-Physical Systems world.

Digital transformation and the optimization of business processes drive organizations to evolve the connectivity between IT and the OT, the industrial control systems. This creates business benefits but it also increases the risk. For some time, we have been at the beginning of an era in which this risk includes loss of life.

The attack on the Oldsmar water treatment facility shows that security attacks on operational technology are not just made up in Hollywood anymore. The world has seen real incidents where events originating in the digital world had an impact on the physical world.

A short glimpse in recent history shows us that attacks on OT are nothing new. Just think about the Maroochi Shire incident in 2000, Stuxnet in 2009 or Industroyer in 2016. A stark example is the Triton malware first identified in December 2017 on the OT systems of a petrochemical facility. Its purpose was to disable the safety instrumented system (SIS) built to shut down the plant in case of a hazardous event. If the malware had been effective then loss of life was highly likely. It is not unreasonable to assume that this was an intended result. Hence “malware” has now entered the realm of **“killware”**

Killware

Many of the attacks we see in the news these days are related to ransomware. The OT environment is not often the prime target of the ransomware – it is more like collateral damage. Unfortunately, we also see more and more attacks on OT environments where the OT is not the objective of the attack, but the means. The actual objective of the attacker is to cause harm to humans by using **killware** in an OT environment. This can be a chemical plant, an air traffic control system, a dam or anything similar.

It just a matter of time before **killware** will have made its first victim, an outcome uppermost in the contemplation of law enforcement agencies. It is likely that by 2025 operational technology environments will have been weaponized to successfully harm or kill humans.

Of course, national governments realized these risks and are creating legislation. The European NIS Directive or the Cybersecurity and Infrastructure Security Agency Act of 2018 in the US are just two examples. There are also standards that organizations use to improve the security of their OT environment: the NIST SP800-82 and the IEC62443.

Most organizations have lived for too long in denial. Risk practitioners are often asked by skeptical executives whether specific risk outcomes have occurred previously.

There has not, yet, been a proven outcome of fatality caused directly by a malicious OT compromise. This is now reasonably foreseeable and **killware** will have made its first victim.