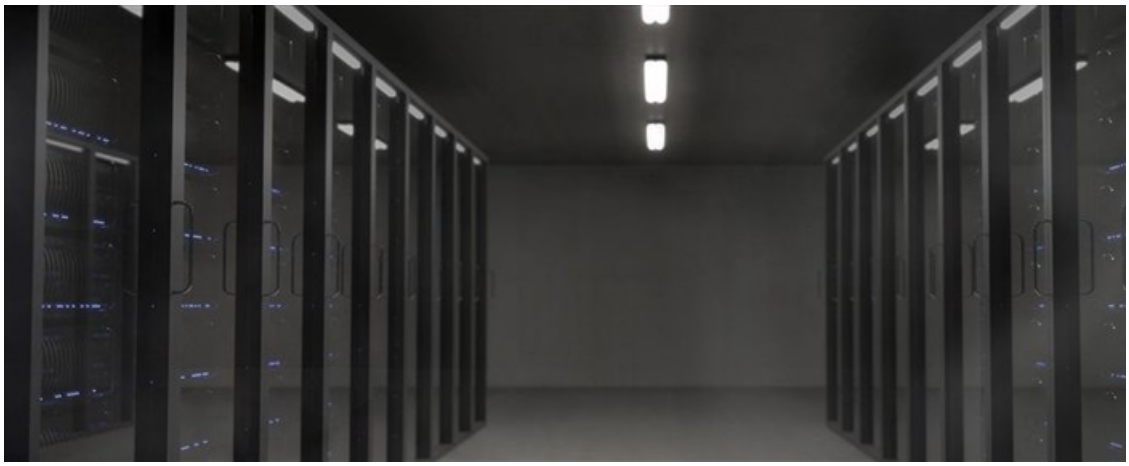
The convergence of IT and OT systems in the mining industry

Digital transformation is disrupting every industry and the mining sector is no exception. However, while emerging technologies offer increased efficiencies, it also opens a host of vulnerabilities that the mining industry has previously not had to worry about.



Source: pixabay.com

In this ever-changing technology-driven world, businesses in all sectors need to be adaptable and put strategies in place to adopt the latest emerging technologies that will help them meet their business objectives.

In the mining sector, technologies like the internet of things (IoT), Artificial Intelligence, cloud technology, big data, Robotic Process Automation (RPAs) have the power to fundamentally change how business is done and introduce efficiencies that will only get better the more they are used – thanks to machine learning.

However, with every introduction of new technology, so a new vulnerability is created. Any business operating within the mining sector needs to ensure that cybersecurity is baked into any new solution brought into their operation.

A look at the 'Mine of Tomorrow'

Colin Blou, VP Global Sales for Claroty spoke at a recent mining round table event hosted by Dimension Data for mining professionals to discuss the 'Mine of Tomorrow' and what mining in the future of our country will look like.

He said that in the past, in the mining sector, machines were monitored by supervisors and processes were manually

managed without any automation. Previously there was also limited to no real-time knowledge on stock levels.

“Nowadays, machines are becoming increasingly automated and interconnected, they are connected to the internet, allowing plants to become connected to each other,” said Blou.

This means that mines can now collect real-time data about stock levels, as well as minimise human safety hazards as machines are tasked with doing the riskier work.
Increasingly in the mining sector, there is a convergence between information technology (IT) systems and operational technology (OT) systems. The two systems are no longer operating in silos but are integrating with one another.

“In an ideal world, there would be a complete segregation between OT and IT networks. However, and as we’ve witnessed along the years, this connectivity happens and exists,” said Blou.

“For example, and as seen with the NotPetya malware attacks last year, IT-centric ransomware affected global companies that neglected to properly segment IT and OT networks. The result was accumulated losses of over $10M for global companies such as Maersk and Mondelez.”

He said nowadays organisations can choose between bad and worse: “Either stay unconnected and not participate in the fourth industrial revolution or increase connectivity which will dramatically increase security exposure and attack surface.”

“The bottom line is the mining sector cannot allow itself to be disconnected so each player needs to decide how to do it in a secure way.”

Blou said there is an asymmetry between IT and OT systems. Within the IT industry, players have been very instrumental in designing and evolving products and solutions to close the security exposure gap.

“From intrusion detection and prevention systems all the way to endpoint prevention and remediation systems, they all have the common goal of keeping things in check.”

Whereas, in the OT industry at the same point in time: “Over the last 30-40 years very minimal efforts have been put in place to protect and consequently minimise the exposure in those networks,” said Blou.

He said this lack of symmetry means integration introduces a weak security posture. Security needs to stay top of mind when creating cohesive systems and Blou said companies should be aware of unpatched devices.

“All too often security tools deliver alerts to the security operation centre without any context surrounding its origin. End-users need visibility into the chain of events leading up to every single alert. This is particularly important for OT security alerts consumed by IT security professionals with limited to no knowledge of OT operations.”