Digging deeper: cybersecurity concerns mount in mining arena

By Kyle Pillay, Security Operations Centre (SOC) Manager at Datacentrix

In today's digital era, the internet's evolution and technologies like the Internet of Things (IoT) have equalised the cybersecurity landscape. No industry, including the mining sector, is exempt from cyber threats such as phishing, ransomware, malware, and financial scams.

In fact, cybersecurity has become a significant concern for global mining operations, with organisations including Alamos Gold, Freeport and others all recently grappling with the aftereffects of some type of cyberattack.

High risk, why risk?

The digitalisation of mining organisations has expanded the attack surface for cyber threats. For instance, cyber attackers might exploit IoT vulnerabilities to manipulate machinery on assembly lines, altering programmable logic controllers (PLCs) that manage various electro-mechanical processes. Such tampering could endanger workers, halt production lines, or even threaten lives, as in cases where heating, ventilation and air conditioning (HVAC) system shutdowns occur due to attacks.

Moreover, the theft and exposure of data where sensitive employees' information was leaked onto the dark web, highlight the severe consequences of cyberattacks. Depending on regional regulations like South Africa's Protection of Personal Information Act (POPIA) or the European Union's General Data Protection Regulation (GDPR), businesses could face significant fines or even imprisonment for lacking adequate cybersecurity measures.

> The digitalisation of mining organisations has expanded the attack surface for cyber threats. For instance, cyber attackers might exploit IoT vulnerabilities to manipulate machinery on assembly lines, altering programmable logic controllers (PLCs) that manage various electro-mechanical processes.

OT versus IT

Operational technology (OT) that is typically used in mines to monitor and control industrial processes is generally manufactured to have a long lifespan. However, today we're finding that these systems, built to last 20 to 30 years and always operated in segregation, are now being increasingly targeted by cybercriminals.

Historically, the OT environment has used the Purdue Model, a structural framework for industrial control system (ICS) security that concerns the segmentation of physical processes, sensors, supervisory controls, operations and logistics, to protect OT equipment

> In this ongoing battle for digital resilience, Datacentrix offers comprehensive services and solutions designed to navigate the complexities of modern mining operations.

from malware and other attacks. However, this model, developed in the 1990s, does not address some of the more modern challenges and requirements of ICS environments, such as the growing interconnectedness of OT and IT, with its broader attack surface, and the ongoing emergence of new, more sophisticated cyberthreats.

Exploring cybersecurity options

To enhance their defence against cyber threats, mining organisations can explore various cybersecurity solutions.

Managing the OT stack with dedicated software can provide some protection and highlight areas for improvement through key performance indicators. Virtual patching and implementing a Web Application Firewall (WAF) can protect application layers while maintaining network segmentation, thus reducing IT risks.

From a data protection point of view, there are several solutions and processes that could be rolled out by mining organisations to assist with the safe gathering and analysing of data from equipment out in the field. For instance, identity access and management (IAM) is key. An IAM solution would ensure that only the right people have access to devices and are able to bring data back into the environment for analysis. Multifactor authentication (MFA) is also critical here, to ensure that users are not being spoofed – where an unknown source poses as a known, trusted source - or impersonated by a cybercriminal.

In addition, safeguarding against insider threats is another critical area to be investigated. Here, data loss prevention (DLP) is critical to circumventing

threats from within the business, motivated potentially by greed or malice, or even just attributed to carelessness. DLP assists with data classification. This type of solution helps to determine data classification; identifying and helping to prevent the unsafe or inappropriate sharing, transfer or use of sensitive data. For example, DLP can determine whether a user is allowed only to upload to a database, or if they may also email it.

In this ongoing battle for digital resilience, Datacentrix offers comprehensive services and solutions designed to navigate the complexities of modern mining operations, helping these organisations to confront the cybersecurity challenges of today and emerge stronger, more secure and better prepared for the challenges of tomorrow.

For more information, please visit www.datacentrix.co.za/security-services.html