Ensure your ERP software is secure in the wake of sophisticated cyber-attacks

By Marius Wessels
Manager, Professional Services
SYSPRO Africa

Image courtesy of freepik.com

There's no question about technology's role in driving business evolution and revolution, but it also creates new layers of cyber-threats to organisations. New technologies are driving up cybercrimes, and businesses should put the proper measures in place to safeguard their enterprise resource planning (ERP) systems against cyber-attacks, which can result in unprecedented and devastating effects.

ERPs, which are at the core of many businesses, house delicate and vital information on everything from customer data, stock levels, order entries, and production plans, to operational processes such as production planning and financial processes such as cash collection and payments. Therefore, their security should be on the forefront of any company's security preparations.

Executives ought to be mindful of how vulnerable their ERPs may be to attacks since attackers are upping their attacking game, shifting from encryption of databases and distributed denial-of-service (DDoS) attacks to disrupting productive systems through attacks that use artificial intelligence and quantum technology. It can only be worse for those using legacy ERP systems without protection.

Some of the top aspects that present cybersecurity risks to an organisation include not knowing the data it has, not knowing which to protect, and not educating the workforce on the dangers and preventive measures to attacks, which can be executed through simple email phishing.

While cyberattacks often result in great losses to business – not only through ransom amounts demanded by the hackers but also downtime and loss of productivity and revenue – it is not all bleak news. There are several ways for companies to ensure their ERP software is cyber secure in the wake of these sophisticated activities by criminals.

Identify the crucial data

The first step to securing an ERP system is identifying the most important data, and where it resides. While many businesses need to be more knowledgeable of their crucial and critical data

and systems, it is of great essence to have a clear view of the data that matters the most, where it is stored, and how it is accessed.

This data is typically stored in various places within an ERP, and it is therefore necessary to track it down to know how to protect it. By doing this, companies will not only be creating a roadmap of how data flows in their system, but also identifying the interfaces involved.

Limit access

It is crucial to ensure that cloud-based ERP shields the web-accessible ERP data from being compromised.

One way of ensuring the data is protected is by exploring your own ERP for vulnerabilities to seal all the loopholes that hackers can exploit.

Also, for these internet-facing ERPs, it is essential to restrict access to the system through a company VPN (virtual private network) connection or firewall. The number of people accessing crucial data points also needs to be limited, to eliminate unnecessary access by employees, which at times proves to be the weak link for attackers.

Additionally, if companies rely on third parties to host or work with their ERP system, it is crucial to ensure they have the best security measures in place. Even with cloud-based security solutions, these companies must be evaluated case-by-case to vet the security measures they employ.

Ensure secure integration

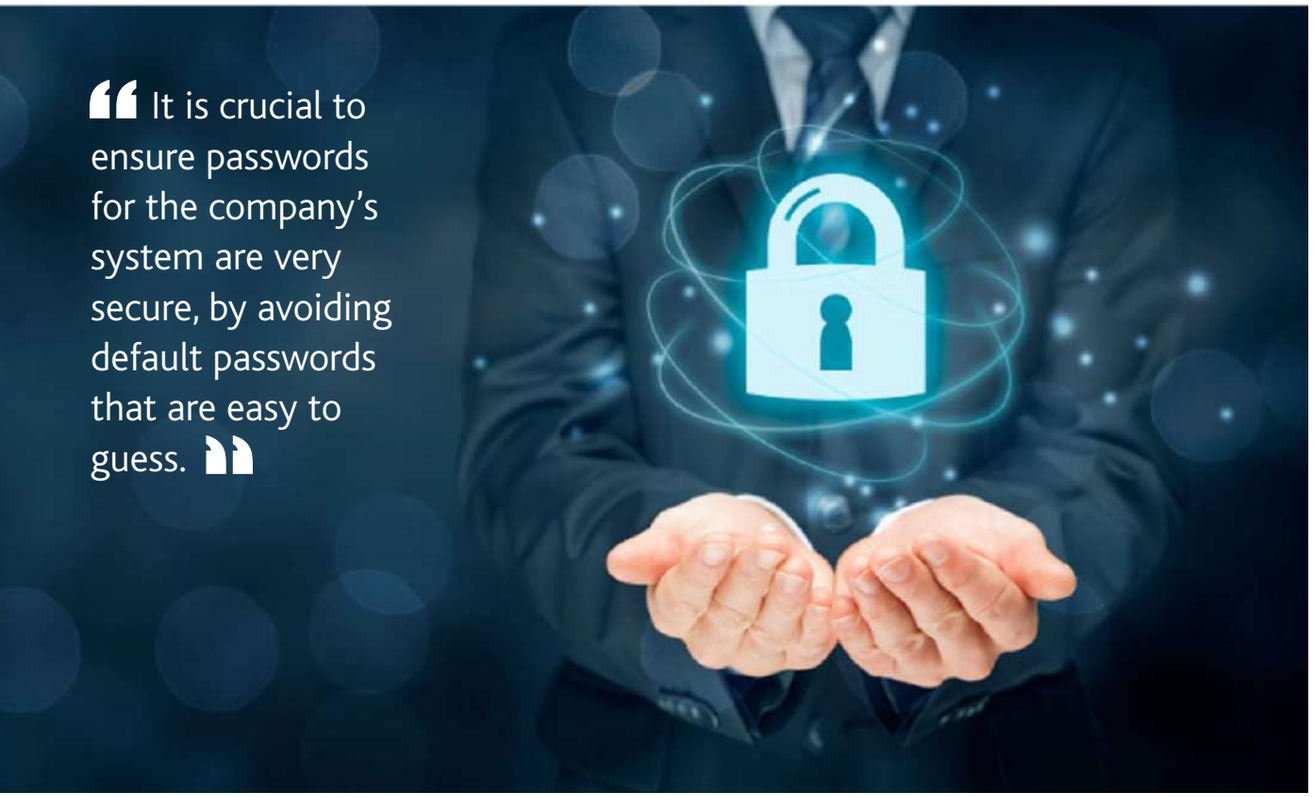
ERP systems are frequently integrated with other applications of an entity. It is, therefore, essential to ensure these integrations are secure. Mapping of the integration interfaces and APIs routinely will ensure that customisation of the system does not compromise security. Here, the organisation could consider installing middleware to reroute the interfaces, enabling easy management of data exchange between the integrations, and making it easy to monitor and shut off when an interface is compromised.

There is also a need for regular assessment of the existing configuration of these interfaces and strong encryption where necessary to prevent data deciphering by hackers in the event of possession. With middleware in place, it can also assist in identifying the unsecure integrations, paving the way for their elimination or remediation, therefore reducing the number of vectors that attacks can emanate from.

Update systems

As aforementioned, cyberattackers keep changing their tactics and developing new ways of executing their malicious activities. With outdated security, an organis ation’s system is more vulnerable and would offer little resistance to attacks. Software developers have a better understanding of the security threats to their applications and tend to address them in the form of software updates.

While many businesses need to learn about updating these systems, owing to their difficulty in updating



> It is crucial to ensure passwords for the company's system are very secure, by avoiding default passwords that are easy to guess.

due to complexity, keeping a system updated comes with enormous benefits.

However, it is more than just the system that needs to be updated. Companies need to ensure they are in the know about current ERP security trends. This involves educating employees on what to look out for and what to do to prevent attacks. Also, it is crucial to ensure passwords for the company's system are very secure, by avoiding default passwords that are easy to guess.

Insure against the risk

With the increased cyberattacks in the recent past, it is only wise for companies to be prepared on how to deal with the aftermath of the event, since there is no guarantee that their system will never be hacked, even with the best security measures in place. Having cyber insurance can help mitigate the destruction caused, ensure quick return to production, therefore the survival of the company. **SR**