

Discover Anything



Read

Write



Drag & Drop Auth For Any App



★ 17,246 reads

How to Protect your ERP System Against Cyber Attacks

July 7th 2022 | by @ameyak

★ 17,246 reads



TLDR



CYBERSECURITY

#cybersecurity

#cybersecurity-writing-contest

#information-security

#erp-software

#business-application




1x

Read by Dr. One (en-US)



Audio Presented by





@ameyak

Ameya Khankar

Receive Stories from @ameyak

name@company.com

SUBSCRIBE

Corporations and governments, throughout the world, have been expanding their reliance on technology to gather, analyze, and store data as the world continues its journey into the digital age. While digital transformations have many advantages for organizations, they have also significantly raised the likelihood of risks. Potential cyber-attacks can be introduced within their digital environments if appropriate risk mitigation strategies are not put in place.

ERP systems: The heart of a business

An Enterprise resource planning (ERP) system is a management information system (MIS) that provides companies with integrated financial, supply chain, and human resource-related functions. These systems allow enterprises to manage several business-critical processes in a single application rather than using multiple different applications that are not compatible with each other.

ERP systems: Key target for cyber attacks

According to a recent report by the US Cybersecurity & Infrastructure Security Agency, cybercriminals are increasingly targeting ERP systems. Below are some recent trends relating to security threats faced by organizations:

Threats	2020	2021
Phishing	~94,000 attacks per month	316,747 attacks in Dec (237% ↑)
Ransomware	1,389	2,690 (92.7% ↑)
Data Breaches	Approx. 1108	1,862 (68% ↑)
Insider Threats	4716	6803 (44% ↑)
DDoS	10 million	9.7 million (3% ↓)

As cyber threats have significantly increased, ERP security controls should be a consistent and ongoing activity in any organization. ERPs may hold sensitive and critical information for businesses (such as financial reporting information, sensitive client data, credit card information, and trade secrets) and therefore ERP security controls should be at the top of each organization's cybersecurity plan.

Protecting your ERP: A unique challenge for the new age business

ERP systems are complex, with multiple components and interfaces. Because of their size and complexity, protecting them is a unique challenge. One of the biggest issues in protecting the ERP system is that many people don't understand how the system works or what makes it special.

For instance, some ERP systems are developed with a lot of custom code and these customizations can be quite complex. An ERP system might have been designed to take orders from high-volume customers and process them in a specific manner. This means that if an attacker is able to hack into the system and steal critical information related to those orders or change key attributes of the order transactions, this will cause significant unwanted business impacts to the organization. Attacks on ERPs due to the complex nature of the systems are often hard to detect unless you know exactly what to look for and/or have developed expertise around the ERP risk landscape.

Steps to guard your ERP system against cyber risks

The first step in protecting your ERP is understanding the risks it faces. Conducting a risk assessment that identifies all potential vulnerabilities should be prioritized. The risk assessment will help identify risks specific to the organization and the ERP application; it can be typically categorized into:

- **External Threats (from outside-in sources):** Unauthorized outside users or threats gaining access to sensitive data residing within the ERP.
- **Internal Threats (sabotage from within orgs):** Insiders or internal threats who could intentionally or unintentionally cause financial damage or steal business-critical data.
- **Application-Specific Risks (human or system):** Application maintenance malfunction or human errors causing unwanted or unintended impacts to the ERP system.

Here are steps to consider for protecting against potential ERP risks:

Develop a security culture

ERP teams are frequently considered as add-ons to cyberattack simulations or are not consulted at all. However, their expertise is required to ensure that the exercises are realistic and key functionality of the ERP system is being

holistically tested.

Building a security culture will be critical in securing the ERP system in the long term. Security culture should be built keeping in mind the strengths and weaknesses of the organization. Employees should be trained on ERP security controls and procedures, and they should be encouraged to report any suspicious activity. ERP administrators should regularly review security logs and monitor for unusual activity.

While these are tactical examples of security culture being implemented, it should be noted that the entire organization should be included in building a security culture. The individuals who must be involved in building a security culture around ERP systems typically are:

- Company's CISO (A person who's responsible for organization-wide IT system security)
- IT Staff (They manage the ERP)
- Finance Staff (They use ERP)

This approach will support employees actively working together to keep the ERP system secure as part of a collaborative security culture.

PRO Tip: *Create awareness about the importance of ERP security controls, and instill a sense of ownership among employees. Consider building a security culture with a top-down approach. Having clear and concise security policies in place and ensuring that all staff members are properly trained in ERP security control procedures will help.*

Identify ERP system interfaces

The creation of an inventory list of all the interfaces between the ERP system and other applications on the organization's network should be considered. This inventory list should not only identify the landscape in which the ERP system operates but should also take into consideration the direction of data flows associated with the ERP systems.

Having documented knowledge around inbound and outbound interfaces is critical information for managing ERP interface security controls as well as scenarios where the ERP system is under a potential attack. Creating this inventory list is a cumbersome process and, depending on existing institutional knowledge, it may involve having conversations with various IT stakeholders and/or application owners to truly understand which components of the IT organizations interact with and impact the ERP system. If there is an existing inventory list already created by another department or during prior system implementation efforts within your organization, use it as a starting point for developing a holistic picture of interfaces.

PRO Tip: *Develop a pilot project where the ERP system owner and other application owners are enabled to discuss, share and document information about how many interfaces exist between the ERP system and other applications. The outcome could be an IT interface landscape chart or diagram which should include the systems involved,*

directional flow of the data, and types of data being processed (including identification of any sensitive information). Use the interface landscape chart for identifying the appropriate level of security controls around ERP interfaces.

Limit user access

Organizations using an ERP system should have a well-designed security controls framework in place that drives ERP security design with the intent to protect its data and prevent unauthorized access around the system. One of the key elements of this security framework should be the concept of least privilege access which means that users should only have access that they need to perform their job duties.

Least privilege access principle should be considered while provisioning users access to the ERP system as well as within the access that is actually provisioned for performing job duties. This can be accomplished by designing roles that appropriately take into consideration the granular security permissions or access rights being granted including adherence to regulatory requirements relating to segregation of duties. Additionally, a risk-based approach to user access can help ensure that only those with a legitimate business need have access to process sensitive data residing in the ERP system.

PRO Tip: *Adopt a risk-based approach to user access. Develop a role-based access control strategy that involves developing custom roles relating to specific activities to be performed by the users. Job function-specific custom roles will also enable in the implementation of segregation of duties. For e.g., create a custom role that can be assigned to junior staff for creating journal entries and another custom role that can be assigned to management for reviewing journal entries (containing only specific permissions required to perform each job). It should be noted that out-of-the-box roles in ERP systems often have excessive access and do not comply with principles of segregation of duties at the security permissions or access rights level therefore having a security control framework that drives the ERP security role design will be key.*

Maintain a process for ERP system changes

ERP system changes can be thought of in two main categories: user-driven changes and vendor-driven changes - both of which might significantly impact ERP security. For user-driven changes, ensure there is an ERP change management process in place. This should involve having a process where changes are requested, appropriately reviewed, and then implemented after adequate comfort is obtained around the change.

For vendor-driven changes, stay on top of vendor updates, patches, and fixes that are released. If the software provider releases a security update, it's likely that they've identified a vulnerability and fixed it. However, remember that not all updates released by the vendor are equal. Therefore, it is essential to have an internal process in place with the right ownership structure where upcoming vendor updates are thoroughly assessed including their impact on the ERP system functionality and security, and then determining whether to apply or reject the update from the vendor. Coordinating with the right stakeholders to assess the impact of the update will be key.

PRO Tip: *Assess what updates are to be released in the future impacting the ERP. Advanced organizations will often consider automating the user-driven change management process through a ticketing system that documents the change requested, segregation between the change requestor and the change reviewer, and appropriate levels of documentation around system testing occurring prior to releasing the ERP system change. For vendor-driven change management, it is critical to coordinate with the vendor to understand their update schedule/frequency and build relationships with the vendor to understand the future change roadmap in order to have enough time to proactively assess and implement the required procedures to maintain the ERP system's security posture.*

Understand the ERP security model

The cloud has quickly become the preferred choice for businesses of all sizes looking to improve their ERP systems. While the cloud comes with a host of benefits, it's important to understand the shared ERP security model before making the switch. In a nutshell, the shared security model means that responsibility for security is shared between the vendor and the customer. The vendor is responsible for ensuring that the physical infrastructure is secure, while the customer is responsible for securing their data and applications. This approach can help you to improve the overall security posture, but it's important to make sure that both sides are aware of their roles and responsibilities.

PRO Tip: *By taking the time to understand the shared security model, one can ensure protection against potential attacks. While many factors go into what security responsibilities are owned by the vendor as compared to the customer, consider the typical breakdown below to assess your ERP security model:*

- *Vendor-owned security: Cloud ERP infrastructures such as physical security, computing, databases, and storage*
- *Customer-owned security: Organizational network elements interacting with ERP systems such as firewalls, identity and access management, application and data security, and customer side authentication and encryption if any*

The above breakdown can also be considered while developing security control ownership between the vendor and customer.

Tactically strengthen ERP system security posture

Multiple leading practice procedures should be considered for strengthening ERP security. This should include: (1) Using threat detection tools (2) Strengthening password policies (3) Implementing two-factor authentication and using virtual private networks (VPN).

In order to keep the ERP system safe from the latest threats, it is essential to invest in up-to-date threat detection and monitoring tool. These tools will scan your ERP system (or associated IT components) for malicious elements and quarantine or delete them if they are found. New threats are constantly being released, so the threat detection tool being used should be regularly updated in order to maintain adequate levels of protection for the ERP system.

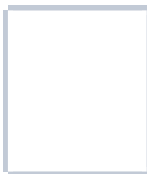
In today's digital ERP age, it's more important than ever to have a strong password policy in place. Passwords are not just used to access the ERP system but also to secure sensitive data stored within it. To protect against unauthorized access, you should set strong passwords with comprehensive password policies (this may include for instance a minimum of 12 characters and include at least one number and symbol).

Two-factor authentication is a user identification method that combines knowledge (something the user knows) with possession (something the user has). The most common example of this is when logging into an ERP system using a username and password and by entering another code sent to a mobile phone or some other device one may own. In this way, additional security is provided, making it more difficult for hackers to access ERP system accounts, even if they have obtained login credentials.

PRO Tip: *While no ERP system security can be full proof, a key element for successfully implementing tactical ERP security procedures is clear ownership of responsibilities combined with up-to-date technical domain knowledge. A dedicated team should be identified for translating organization-wide security policies into everyday tactical ERP security measures. This team should be empowered with the right technical knowledge through training, awareness, and culture-building and should be set up for success by providing them the right foundation for building organization-wide relationships for long-term ERP cybersecurity success enablement.*

Conclusion

Any business that relies on ERP systems needs to have a strong security posture in place as these systems are often critical for business operations. Because ERP systems are designed to give businesses a 360-degree view of their business, they can be more vulnerable to security threats. It is important for businesses to understand the potential risks around their ERP systems by identifying internal and external threats to take appropriate steps to mitigate them. By considering leading ERP security practices, staying on top of ERP security threats, and having monitoring mechanisms in place, cybersecurity threats around ERP systems can be potentially reduced.

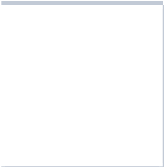


by Ameya Khankar [@ameyak](#).

[Read My Stories](#)

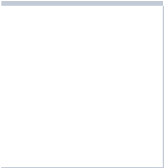


RELATED STORIES



184 Stories To Learn About Psychology

Published at Oct 03, 2023 by [learn](#) [#psychology](#)



Global Celebration Marks International Ethical Hackers Day on October 1st

Published at Oct 03, 2023 by [eccouncilofficial](#) [#ethical-hackers-day](#)



The Prisoner's Dilemma.

Published at Oct 02, 2023 by [suelettedreyfus](#) [#non-fiction](#)



Maximizing Value FP&A With Enterprise Planning Management

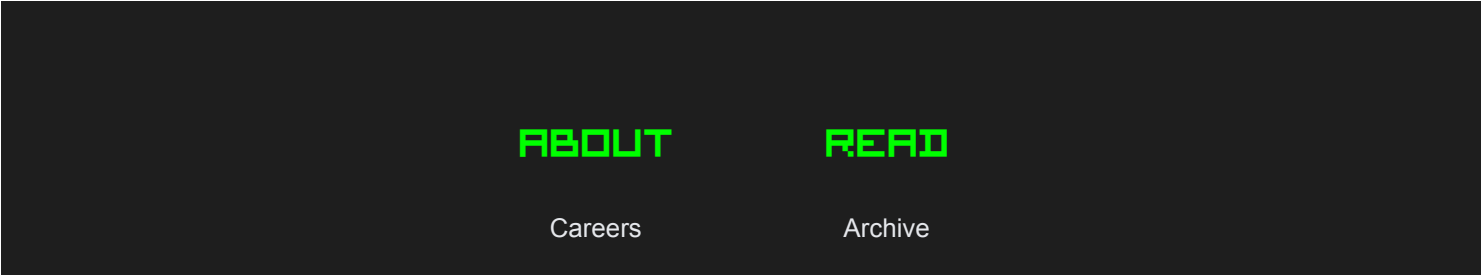
Published at Oct 02, 2023 by [polestarsolutions](#) [#business](#)



Beyond Deleted: Cradle's True 'Disappearing' Message Technology.

Published at Oct 02, 2023 by [ascend](#) [#cybersecurity](#)

LOADING
... comments & more!



Contact	Categories
Cookies	Image Gallery
Emails	Leaderboard
Help	Learn Repo
Privacy	Noonification
Sitemap	Signup
Shareholders	Tech Beat
Startups 2023	Tech Brief
Testimonials	Tech Tags
Terms	Terminal Reader
Updates	Top Stories

WRITE

PARTNER

Distribution	Billboard
Editor Tips	Book Demo Meeting
Guidelines	Business Blogging
Help	Case Studies
New Story	Company Directory
Perks	Crypto Directory
Process	Live Business Posts
Prompts	Newsletters
Subscribers	Niche Targetting
Story Templates	Partnerships
Testimonials	Startup Package
Why Write	Writing Contests

THE HACKERNOON NEWSLETTER

Quality Reads About Technology Infiltrating Everything

name@company.com

Subscribe

☐ Yes, I agree to receive electric content at Noon by HackerNoon



Get our mobile app on
App Store



Get our mobile app on
Google Play

© 2023 HackerNoon. All rights reserved - PO Box 2206, Edwards, Colorado 81632, USA

