Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 04, April-2020

Evolution of ERP Cybersecurity

Rishit Mishra
Security Manager,
Pricewaterhouse Coopers (PwC)

***Abstract*—When we think of Cyber attacks or Cybersecurity the Enterprise Resource Planning or ERP applications of an organization never come to our mind. This is strange given that the ERP applications hold some of the most important data, sometimes referred to as “crown jewels” within them. So, it should not come as a surprise that within the last few years ERP systems have become a lucrative target for cyberattacks.**

Keywords*— *Enterprise Resource Planning(ERP), Cyberattack, Cybersecurity, Security

WHAT IS AN ERP?

An ERP or an Enterprise Resource planning solution is a business process management system or software that helps an organization integrate its most important applications or business functions/processes and automate many back-office functions. This includes finances, customer accounts, HR, marketing operations, sales and distribution etc. Most knows examples of ERP’s are SAP and Oracle EBS.

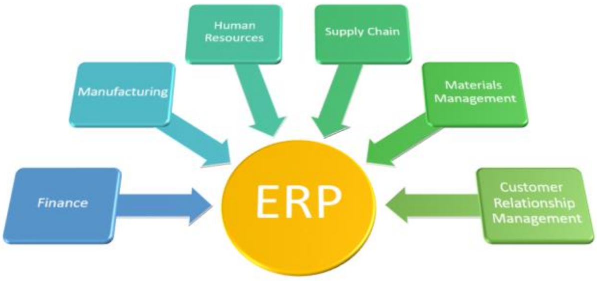

Image 1 – ERP System

WHY TARGET ERP SYSTEMS?

Think of ERP systems like our human heart. The ERP systems bring together various departments within an organization such as accounting, warehouse, inventory, HR so that they function as one unified entity. Since these departments now work together there is seamless flow of data between the departments which is generally stored within a common database hence making the impact of the compromise much bigger.

It is by design the ERP systems store very critical data such as personal identifiable information (PII) data of their employees and customers, financial information, proprietary formulas etc. making them a lucrative target for cyberattacks.

Given the criticality of data the ERP systems store there must be robust security measures that should be put in place to safeguard this information. Often these essential safeguards are not in place making ERP systems vulnerable to attacks and industry experts are saying that the attacks are the rise. Hence it is imperative that when companies are planning their future strategy, they do think of cybersecurity as an investment and not just brush it aside as an expense.

WHY ARE ERP SYSTEMS LEFT UNPROTECTED?

One of the main reasons that why the ERP systems are not as secure as they should be is the lack of understanding of the risk from the business or stakeholder community. Part of the problem is the inability of the IT team to effectively communicate the risk to the business in a method that would make it easy for them to understand. The IT teams a lot of the times project to the business teams very technical results and seldom communicate as to how the cyberattack impacts the day to day functionality of the business. They fail to communicate the impact the downtime of the systems will have, the loss of confidence the customers will see if the company is attacked and how the brand value of the company will get diminished. The IT teams are basically not able to weave this into the business strategy and hence the risk is seldom understood or addressed by the business leadership. This results in potential areas of vulnerabilities not getting identified which the attackers exploit to gain unauthorized access to the system.

Also, a lot of the companies try to address this more as a reaction or after the fact after they’ve been attacked rather than proactively taking actions to secure the system. They come into action after an attack has occurred and at that time start scrambling to find out why an attack happened rather than protecting the system before hand against any form of attacks.

As companies move to the cloud and encourage BYOD (bring your own device) we see users accessing systems across multiple platforms. Now if any of the platforms are compromised it is easy for the attacker to gain access unauthorized access to the ERP system. Another thing that is observed is that smaller companies think they are not on the radar of the cyber attackers and the cyber attackers are only interested in targeting bigger companies, whereas it has been found that over 60% of the cyber-attacks were against smaller companies. Being small, the companies have limited budget overall and hence they tend to rely on security solutions provided by their ERP providers.

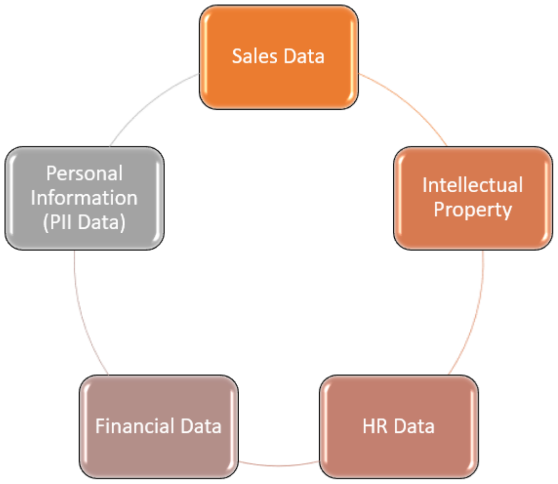

Image 2 – Type of data leaked when ERP systems are compromised

Lastly it was also observed that there is lack of ownership when it comes to securing these ERP applications. Generally, there is a dedicated team that does take care of security within the ERP applications and is responsible for compliance related issues which are part of the yearly audit. But when it comes to securing configurations, network, securing the application layer, database layer etc. it's the responsibility of another team. Now the two teams should actually be working closely to determine the proper security measures to put in place but that seldom happens. Another thing that is observed is that companies willingly compromise on security to gain efficiency on performance. That's a typical behavior that even we in our personal lives do like using a faster or a lighter antivirus just so that our computer is faster.

HOW TO PROTECT YOUR ERP SYSTEMS?

One of the most important security concepts is defense in depth which means that its not one solution that is the answer, but multiple solutions put together which solve the problem. Think of multiple traps set in place to protect a treasure instead of just one trap. Same applies for ERP security. Its working of all these efforts together that results in a security ERP and overall a secure organization.

A. *Keep your system patched and up to date*

Like we do for our computers, like when windows introduce a new software upgrade or security patch, we rush to upgrade our system to that our system is not attacked and our personal data not compromised. In the same way its critical that our ERP systems are up to date and critical security patches are applied to them in a timely manner. US CERT which is part of the Department of Homeland security has issued multiple alerts for SAP over the past couple of years. US CERT Alert (AA19-122A) highlighted that SAP systems were susceptible to attacks due to vulnerabilities that have been in the systems for decades. Now SAP had released patches which would take care of this vulnerability years ago but there were a lot of companies that had not put the required patches in place.

SAP has something called "**Patch Tuesday**" where they release patches on the second Tuesday of every month which help fix vulnerabilities that have been detected in SAP products. Now this will also make cyber attackers aware that the vulnerabilities exist. Hence the companies that do not apply the patches quickly, fall victim to these attacks.

In addition to keeping your ERP up to date it is also important to keep the devices you use to access the systems up to date. As mentioned as more and more users are using multiple ways to access the system, there is increased need to protect every avenue. If any of the methods are compromised, it poses a risk to the entire ERP application.

B. *Employee Training*

As the number of cyberattacks have been increasing over the years, the companies are trying to learn from the mistakes and do a root cause analysis as to what was the main reason that the attack happened. It was seen that humans were the leading cause of cyber-attacks. Social engineering is one of the easiest methods used by cybercriminals to manipulate humans and dupe them into falling their trap. Think of phishing emails like the ones we get which say "You've won a lottery" or winning a vacation somewhere exotic or that your bank account has been compromised and you need to login immediately. These are common traps which are used to exploit the human nature and no matter how many security protocols you spend on if the employees are not educated on how to be wary of these attacks the protocols will prove to be completely futile.

Frequently having these security trainings and making sure the security trainings are something the employs understand is key. Even if you make the trainings mandatory or make them as part of the employee's performance review it does not guarantee that the training is being done sincerely and that the techniques taught in the trainings are being applied. Additionally, employees need to be made aware of the importance of using strong passwords. A lot of times the password of a person is their date of birth, mother's or father's name, place of birth etc. which are easily cracked by hackers. Using strong passwords which are a combination of letters, numbers and special characters should be used.

C. *Incident Plan & Response*

One cannot stress enough the importance of the incident and response plan. Just like we often say be prepared for the worse, same way it is key to have a solid incident and response plan. The plan highlights the steps to be followed in case a cyber-attack happens and identifies the roles and responsibilities of the individual people in case of an attack. This is very crucial since it helps to have a clear understanding of who needs to do what at such a critical time.

D. *Use Encryption*

As companies are become more and more flexible with their employees and promoting work life balance, we see a lot of employees working from home. It is easy to protect and strengthen the network the employee is using when they are in the office but now as more and more people are connecting from their homes encryption plays a very big role and will be the key to protecting the company's ERP system.

E. *Private Cloud*

Since the advent of cloud technologies there's always been a debate on whether going public, private or hybrid is the best bet. From the beginning the private cloud has been the most expensive but are the most secure. For systems like ERP's which store some of the most critical data within the system it makes sense to go with private clouds.

SUMMARY

As addressed here ERP systems are critical for functioning of day to day businesses for an organization. A compromise to an ERP system because of a cyberattacks can cripple the organization and the impact of it are far reaching than just economic. Hence it is necessary to take the required precautions to ensure that the ERP systems are secure.

REFRENCES

[1] https://api2cart.com/business/how-cybersecurity-involved-in-erp-systems/
[2] https://securityboulevard.com/2019/05/what-does-the-second-us-cert-alert-of-2019-mean-for-you/
[3] https://www.us-cert.gov/ncas/alerts/AA19-122A
[4] https://www.cybersecurity-insiders.com/dhs-says-erp-systems-are-vulnerable-to-cyber-attacks/
[5] https://www.sagesoftware.co.in/blogs/erp-and-cybersecurity-what-no-one-is-talking-about-2/
[6] https://www.panorama-consulting.com/the-importance-of-investing-in-cyber-security-as-part-of-your-erp/