TITAN

CONSULTING

IS YOUR SAP ENVIRONMENT SAFE AND SECURE?

Align Your Security Strategy and Practices!

"I'm sorry sir, your charge was declined, do you have another credit card?"

I was embarrassed…and upset. I had just paid off the card - what happened? I called the credit card company, and they politely told me the problem. *"Sir, we believe your card has been compromised. We don't believe that your data was stolen. As a precaution, we sent you a new card!"*

This is the 3rd credit card in two years that has been compromised. Security breaches are happening at an alarming rate. If hackers and identity thieves are robbing banks, what are they doing with your SAP data?

Hackers are successfully going after SAP data and for a good reason:

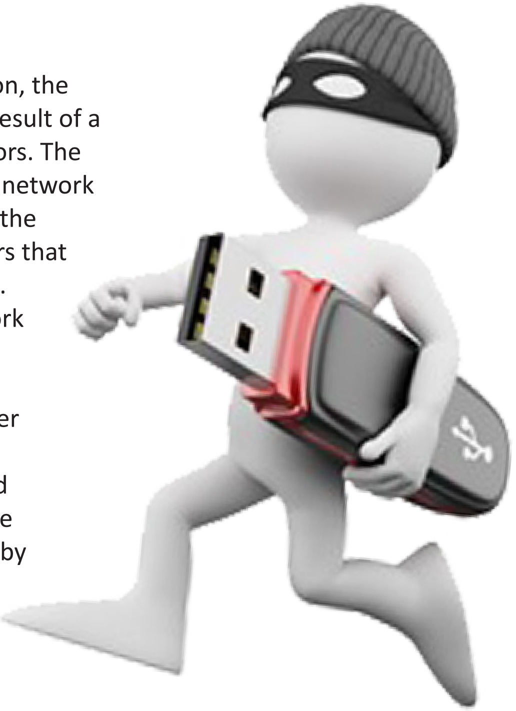
- 74% of global revenue touches a SAP system.
- 87% of SAP's customers appear on the Forbes Global 2000.

Recently, a breach occurred and forced a company to file for bankruptcy protection. The company, a federal contractor who performs background checks for DHS, was hacked by Chinese-sponsored hackers.

The breach occurred, and 25,000 Department of Homeland Security's HR records were compromised. The records, hosted by a 3rd party, contained personal and potentially compromising information. The contractor lost $2.8 billion in federal contracts, 2,500 people lost their jobs, and the company filed for bankruptcy. All this was a result of not protecting their SAP data and endpoints.

This is one example of the devastating impact of the intentional theft of your confidential and proprietary data. There are many methods for perpetrating these crimes. The most common methods where SAP data could get compromised are:

- Access through Suppliers and Vendors
- Outsourced Processes and Applications
- Networks, Middleware (NetWeaver) and Endpoints: Mobile Devices, Tablets, PC's
- ABAP and Custom Applications



In the above situation, the vulnerability was a result of a combination of factors. The hackers infiltrated a network belonging to one of the contractor's suppliers that stored ERP software. The partner's network was connected to the contractor's network. The attacker navigated from the third-party-managed environment into the company's network by successfully brute-forcing a password on an application server.

Once the attackers logged into that server, they installed a malicious backdoor that allowed access to the personnel records. Patience and time are on the side of the hackers unless you have a comprehensive strategy in place and execute it.

The office of the Chief Information Security Officer (CISO) is challenged to prevent these thefts and protect the fiscal health of the company. SAP systems are one of their principle areas of focus since the corporate data jewels reside in SAP. Your customers, pricing strategies, pricing values, your products, sales figures, and trends reside in your ERP systems.

From the PriceWaterhouseCoopers CEO Survey, cyber-crime is one of their top concerns. Most companies have a CISO and Strategy for cyber-security. How does SAP fit into this strategy?

Breaches are frequently traced back to business partners; vendors that may not have the size or capacity to enforce security protocols. Recently, malware was introduced by a vendor into a global manufacturer when it was attached to data shared across their network.

Middleware like NetWeaver is a target for attacks. Cyber-thieves targeted NetWeaver in 2014 by analyzing traffic patterns and stole customers banking information. SAP fixed the exposure via patches, but an alarming statistic with hackers is they are patient: they can lie dormant for more than 100 days before they begin to perpetrate their crimes.

In SAP's defense, they fix these vulnerabilities as soon as they are aware of them. However, customer's practices also are to blame. They do not upgrade the latest patches (OSS Notes). This is relevant to SAP customers that moved off SAP support to any 3rd party software maintenance providers.

Since 2012, SAP has generated over 3,500 OSS notes specifically related to security. Every month on SAP Critical Patch Day (every second Tuesday), SAP releases one or more internal advisories called SAP Security Notes. Such an advisory usually stores information about one or more vulnerabilities found in SAP products or misconfigurations that bear some risk to SAP systems.

SAP has many tools to help IT departments thwart and detect possible breaches and vulnerabilities. At a recent ASUG Executive Exchange that we sponsored, Anne Marie Colombo presented SAP's Approach to Safeguard Your Business. You can find the link on our website: https://www.titanconsulting.net/saps-approach-to-safeguard-your-business/

Our recommendations related to protecting your SAP systems:

1. Audit your systems and applications for potential risks and vulnerabilities.
2. Confirm the security practices and protocols with your 3rd parties and partners – and make them liable for breaches.
3. Review custom applications, development and GUI's for vulnerabilities.
4. Investigate and monitor access and endpoints at all locations.
5. Apply Patches and OSS Notes frequently.

Is your data safe? Do you have good security practices? Titan Consulting is a leader in slashing IT costs and risks. If you have questions about Security Best Practices or how to improve your policies and procedures, Contact Kent Lamb, kent@titanconsulting.net, 214-632-5621; or your Titan Consulting Sales Director.