

RSACONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Too Critical To Fail *Cyber-Attacks on ERP, CRM, SCM and HR Systems*

SESSION ID: HTA-R01

Mariano Nunez

CEO

Onapsis Inc.

@marianonunezdc



Why Should We Care?

*Over 95% of the ERP systems analyzed were exposed to vulnerabilities enabling **cyber-attackers to take full control of the Business.***

*In 100% of the cases, information regarding those vulnerabilities had been **in the public domain for more than 5 years.***

Agenda

- ◆ Introduction
- ◆ Measuring Risk: Reality Check
- ◆ A False Sense of Security
- ◆ Live Demo: Attacks on ERP systems over the Internet
- ◆ The Responsibility Gap
- ◆ Live Demo: APTs and ERP systems
- ◆ Protecting your Business

RSA CONFERENCE 2014

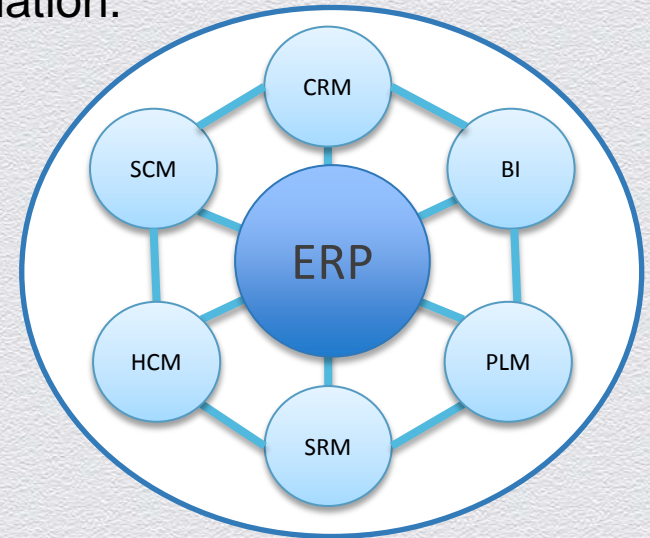
FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



Introduction

Business-Critical Applications

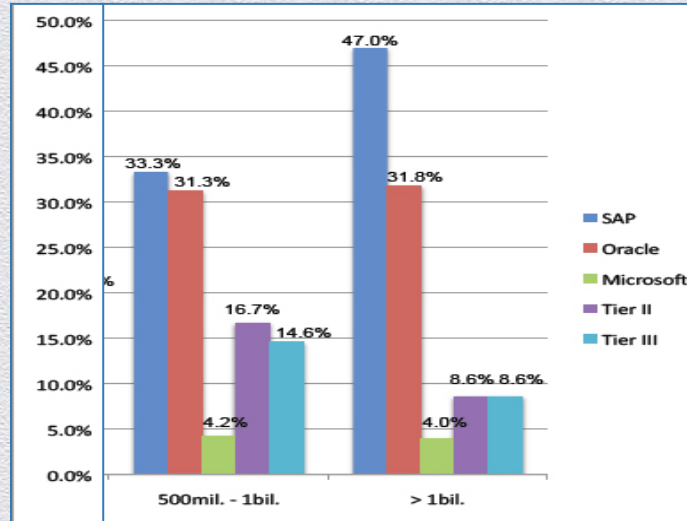
- ◆ The applications that build up the Heart of the Business.
 - ◆ They store our most critical business information.
 - ◆ They run our most critical business processes.
 - ◆ Our day-to-day operations are highly dependent on their availability.



Which Platform(s) are you Running?

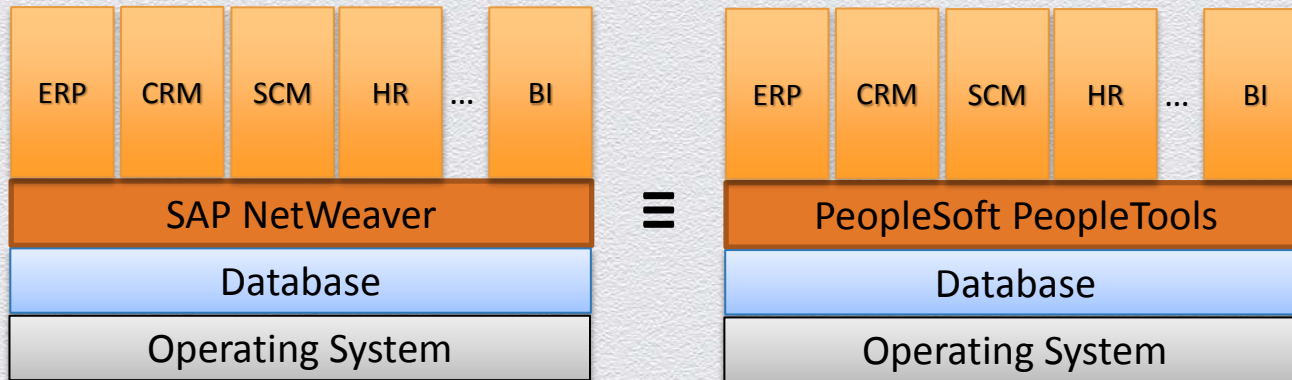
- ◆ Implementations in large Organizations are dominated by two vendors:

- ◆ **SAP**
- ◆ **Oracle**
 - ◆ E-Business Suite
 - ◆ PeopleSoft
 - ◆ Siebel
 - ◆ JD Edwards



Complex, Cross-Module Proprietary Frameworks

- ◆ SAP and Oracle business solutions run on top of a common (proprietary) technological framework.
- ◆ You can think of this framework as the OS, and the business solution/module (ERP, CRM, etc.) being just an “app”.



RSACONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



Measuring Risk: Reality Check

Attacks on Business-Critical Platforms

- ◆ **Why would someone attack our ERP, CRM, SCM or HR systems?**
 - ◆ **Because of the Information they store**
 - ◆ Manufacturing recipes, HR data, credit cards, financial results, etc.
 - ◆ **Because of the Processes they run**
 - ◆ Procurement, Manufacturing, Logistics, Sales, Payroll, etc.
 - ◆ **Because of our Dependence on them**
 - ◆ Interfaces with payment gateways, SCADA/ICS, Govt. entities, etc.
 - ◆ Employees use these systems for their everyday work.

What could be the Impact?

- ◆ **Espionage**

- ◆ How much would the information stored in our ERP systems be worth to our biggest competitor?

- ◆ **Sabotage**

- ◆ How much money would we lose if our ERP system is taken offline continuously, for several hours or even days?

- ◆ **Financial Fraud**

- ◆ What would be the economic impact if someone is able to manipulate all of our financial information and processes without any kind of restrictions or controls?

From the Trenches: Impact Analysis (Sabotage)

- ◆ *“The information coming out from our SAP platform is used to stamp a government-seal in our products in the production line. If we lose connection for more than 2 minutes, we are forced to throw away the entire production for that day” – SAP Security Lead, Global 100*
- ◆ *“We process over \$40,000,000 during the weekend through a Web Service running on top of our externally-facing SAP system” – Security Architect, Global 100*
- ◆ *“If our SAP system was taken offline, that would cost the company **\$22,000,000 per minute**” – CISO, Fortune 1000 (Food & Beverage)*

What is the Probability? Killing Some Myths

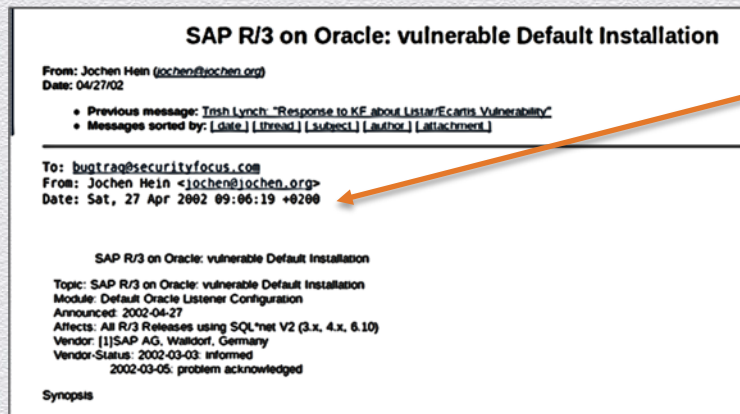
- ◆ **“My ERP platform is only accessible through internal networks”**
 - ◆ There is no such thing as an “Internal” Network anymore. There are no more “perimeters” (spear-phishing, rough contractors, malicious employees)
 - ◆ Many ERP systems are directly connected to the Internet (Web apps, Mobile, cloud-deployments, etc.)

Finding ERP systems through Google Dorks

<code>inurl: /forms/frmservlet</code>	(E-Business Suite)	<code>inurl: /jde/E1Menu</code>	(JD Edwards)
<code>inurl: /OA_HTML/OA.jsp</code>	(E-Business Suite)	<code>inurl:/jde/share</code>	(JD Edwards)
<code>inurl: callcenter_enu</code>	(Siebel)	<code>inurl:/irj/portal</code>	(SAP)
<code>inurl: esales_enu</code>	(Siebel)	<code>inurl:/logon/logonServlet</code>	(SAP)
<code>inurl: start.swe</code>	(Siebel)	<code>inurl:/sap/bc</code>	(SAP)
<code>intitle:"PeopleSoft Enterprise Sign-in"</code>	(PeopleSoft)	<code>inurl:/scripts/wgate</code>	(SAP)
<code>inurl: /EMPLOYEE/HRMS/</code>	(PeopleSoft HR)		

What is the Probability? Killing Some Myths (cont'd)

- ◆ “This can only be performed by highly-skilled attackers”
 - ◆ Who is the Threat Actor? Most likely an **unethical competitor, disgruntled employee, hacktivists or foreign state.**
 - ◆ Even script kiddies – **the information is out there!**



Date: Sat, 27 Apr 2002

What is the Probability? Killing Some Myths (cont'd)

- ◆ **“Our ERP system has never been hacked”**
 - ◆ Less than 5% of the systems we evaluated have the basic Security Audit Log enabled, and just for compliance reasons.
 - ◆ Even with the standard Security Audit features enabled, attacks to the technical layer may not be detected.
 - ◆ Furthermore, is someone reviewing those logs?

So... probably the most honest answer is: “we don't know”.

What is the Probability? Killing Some Myths (cont'd)

- ◆ **“There are no well-known attacks reported against these systems”**
 - ◆ Nov. 2007, students charged with hacking PeopleSoft to fix grades.
 - ◆ Oct. 2012, Anonymous claimed intent to exploit SAP systems.
 - ◆ Nov. 2013, a malware targeting SAP systems discovered in the wild.
 - ◆ Jan. 2014, Chinese hacker published an SAP vulnerability in the Internet-facing SAP NetWeaver Portal of a brand-name Semiconductors company.
 - ◆ *2007-2014, several (non-public) SAP security incidents reported to Onapsis.*

So, What's the Real RISK?

The Probability is definitely not Low.

*Even if we like to think so, **the Impact component may be simply too high to be ignored.***

State-Sponsored Attacks & ERP Systems

- ◆ On Feb 12th 2013, President Obama issued an Executive Order on Cybersecurity – “Improving Critical Infrastructure Cybersecurity”
- ◆ The EO defines *Critical Infrastructure* as:

“systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, **national economic security**, national public health or safety, or any combination of those matters.”
- ◆ *What would be the Impact to the national economy of a large-scale attack to the ERP systems of the Fortune 100 companies and military organizations?*



RSACONFERENCE2014


FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO

Live Demonstration

**Attacks on ERP systems
over the Internet**

RSACONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



A False Sense of Security

But we have an ERP Security Team!

- ◆ Several years ago, ERP Security was only about securing the business modules through Segregation of Duties (SoD) controls (aka. access controls / strict user authorizations).
- ◆ Every large organization today does have an “ERP Security Team”.
- ◆ Therefore, many organizations ***believed*** that they were addressing the problem by having a dedicated ERP Security Team enforcing SoD controls. **This created a false sense of security, as these controls were not designed to prevent/detect cyber-attacks.**

The Evolution of the Threat

- ◆ While SoD controls still apply, underlying technological frameworks handle key security aspects: authentication, auditing, interfaces, remote services, etc. **The security of this technical layer has been overlooked.**
- ◆ Therefore, attackers evolved -> “let’s now target the technical layer”:
 - ◆ Exploits and attack vectors are cross-business-module for a target platform
 - ◆ No valid user required (!)
 - ◆ Attack results in high privileges (!)
 - ◆ Lack of audit trails or proper detection mechanisms (!)

RSACONFERENCE2014

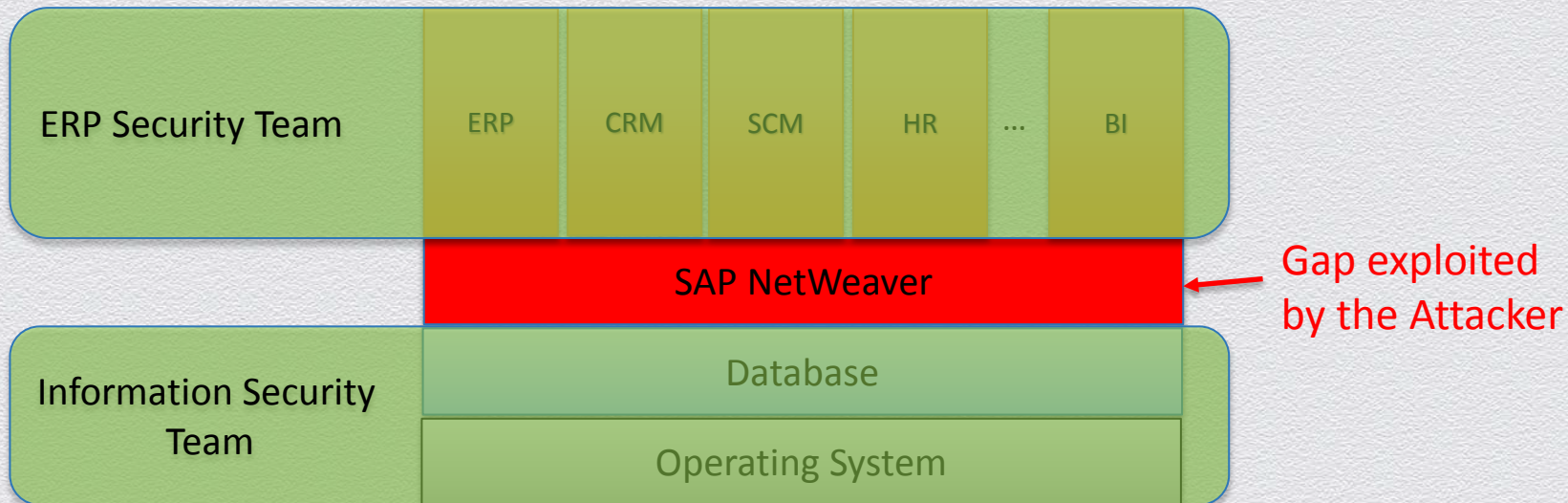
FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



The Responsibility Gap

Who's Looking after these Threats and Attacks?

- ◆ In some Organizations: ***still nobody.***



The Responsibility Gap

- ◆ ERP Security Teams know nothing about hackers, zero-days or malware.
- ◆ Information Security Teams know nothing about ERP systems.
- ◆ **Who's then responsible for preventing these attacks?**
- ◆ Another way to find an answer:

“Who will Executive Management blame in case an attacker breaks into my ERP platform, exploiting a vulnerability disclosed at DEFCON 5 years ago?”



RSACONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO

Live Demonstration

APTs and ERP systems

RSACONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



**Protecting your
Business**

Closing the ERP Cyber (In)Security Gap

- ◆ The ERP Security / Operations Teams must be responsible for properly securing the systems (incorporating secure configuration and security patch management to their current practices).
- ◆ However, Information Security must be the objective 3rd party that can assure to the Business that these Teams are properly doing so. Furthermore, Information Security must be monitoring the systems for traditional and application-level attacks.
- ◆ In short: Apply the old principle of “**Trust, but verify**”.

Take-away: A 5-Step Approach to Closing the Gap

1 – Inventory

Which are our business-critical systems and who are their Business and IT owners?

2 – Assess

What is our current exposure? Which best-practices are we following to prevent cyber-attacks to these systems (beyond SoD)? Who is responsible for applying them?

3 – Plan

Which is our Risk tolerance? Which kind of Risks are we going to address and Why?

Who is going to be responsible for managing these Risks?

Take-away: A 5-Step Approach to Closing the Gap

4 – Enforce

Who is now responsible for ensuring the current Risk level is acceptable with the Business?

5 – Monitor and Adjust

Are there gaps between the current and desired state? How do we fix them?

Have we been attacked? How were those incidents managed?

RSACONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



Conclusions

Wrapping Up

- ◆ ERP, SCM, CRM, HCM, BI and PLM are probably some of the most critical platforms of your Business. However, due to a false sense of security and a responsibility gap, they are highly likely exposed to cyber attacks.
- ◆ The Risk is significant – the Impact component is too High and many systems are still vulnerable to issues known for several years.
- ◆ The Responsibility Gap puts InfoSec teams in a difficult situation – they are not empowered to secure the systems, but it is highly probable that they will be held responsible in the face of a cyber security breach. We need to Close the Gap.