KEEPING INDEPENDENTS AHEAD OF THE CYBER THREAT

Mario Chiock, CISSP, CISM, CISA
Tweeter: @chiock
AGENDA

• What do Oil & Data have in common?
• Sample of Attacks in the Oil & Gas
• Cyber Threat – Statistics
• Technology alone is not the solution
• Cyber-security is the responsibility of everyone
• Cyber Threat – Essentials
• Takeaways
WHAT DO OIL & DATA HAVE IN COMMON?
WHEN SPILLED … BOTH CREATE A BIG MESS

DATA Spilled on the internet
A fellow Houston InfraGard member in the energy sector shared the following information:

It looks like some unknown actors have managed to compromise www.seg.org/amhousing. SEG is a perfect target if your ultimate goal is the energy sector. We already had 20 of our folks receive a phishing email pointing that to that link. The phishing email header also contains the domain exacttarget.com.

Phishing directed users to:
www.seg.org/amhousing Page
This page redirected to a Page that had:
Nuclear Exploit Kit
&
RIG Exploit kit
Taking control of the machine of the users clicking the link
Approximately 300 oil and energy companies in Norway have been hit by one of the biggest cyber-attacks ever to have happened in the country. “Spear phishing attacks – increasingly through the compromised systems of small suppliers to large companies— is an increasingly interesting attack vector for criminals attempting to steal valuable information and IP”.

http://www.theregister.co.uk/2014/08/27/norwegian_oil_hack_campaign/
SAUDI ARAMCO - SHAMOON

- +30,000 machines
- Insider Exploiting privilege account
- Use of default passwords
- Use of shared accounts

- Khalid A. Al-Falih, CEO, email info as follows:
  Khalid.falih@aramco.com  password:kal@ram@sa1960
OTHER CYBER ATTACK TO OIL & GAS

Malware on oil rig computers raises security fears


Exxon, Shell, BP hacked in Night Dragon attacks

HACKERS BREAK INTO CORPORATE SYSTEMS THROUGH VENDING MACHINES AND ONLINE RESTAURANT MENUS


Hackers Break into Corporate Systems through Vending Machines and Online Restaurant Menus

With firewalls ever more difficult to breach, hackers have found other ways to sneak into protected computer systems, even those involving restaurant menus and soda machines.

When an employee uses his or her company computer to order food through an online menu, they can open up a cyber door for intruders to slip through and gain access to the local network of servers.

That’s what happened to one unidentified oil company, The New York Times reported, when hackers attached malware to an online menu belonging to a Chinese restaurant frequented by the oil firm’s employees. Simply browsing the menu resulted in the malicious code downloading into the user’s computer and on to others at the corporation.

Vending machines set up in company break rooms also can provide a backdoor into a supposedly secure network. Many such machines contain minicomputers that allow the vendor to remotely check on the supplies of soft drinks. But the same system can be utilized by hackers to infiltrate the computers of the company hosting the vending machines.

Printers, thermostats and videoconferencing equipment can also be vulnerable to intruders.

In other cases, hackers break in through a third-party’s computer system, such as those providing heating and air conditioning at an office. This happened to retailer Target, which had its payment card system breached, potentially costing the company up to $420 million.
Phishing still hooks energy workers

Posted on December 22, 2013 at 6:30 am by Zain Shauk in Premium, Safety/Security

HOUSTON — The largest energy companies want their workers to stop clicking on links to cut cat photos.

Such emailed links are among the leading ways that hackers gain access to energy company systems — a trick known as phishing, with the potential for breaches that could lead to huge thefts of data, or even physical damage.

Phishing attackers try to get computer users to click on a link or download an attachment in an email that allows hackers to enter their systems.

In their latest counterattack, Schlumberger, Shell and other major players in the energy sector have been sending their employees fake phishing emails.

Unfortunately for many companies, employees are easily coaxed into clicking on bad links, said Jim Hansen, executive vice president for PhishMe, which specializes in phishing risks.

“Something as foolish as silly pictures of cats,” Hansen said. “You think it’s not going to happen. It always happens.”

(Fotolia for Frances)
CYBER THREAT – STATISTICS

• 70% of Breaches are found by 3rd parties
  • Law Enforcement
  • Other investigations
  • Partner or customer
  • others

• 74% of Breaches where not detected in months

• 5% of Breaches were not detected over a year

• Method of attack
  • Phishing
  • Vishing
  • Malware
  • 3rd Party - Insider

• 85% of incidents successful in minutes

• Most Frequent Cause of Breaches: Negligence - 41%

• 50% data successfully exfiltrated in few hours

Many companies been breach just don’t know it yet

Source: 2013 Verizon Data Breach Investigations Report & Ponemon Institute
**TECHNOLOGY ALONE IS NOT THE SOLUTION**

<table>
<thead>
<tr>
<th>Prepare</th>
<th>Prevent</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
<th>Lessons Learned</th>
</tr>
</thead>
</table>
| **People** | • Training ● Awareness ● Experience (Skills) ● self phishing  
• Responsibility & Accountability for cyber security (Everyone) |
| **Process** | • Policies & Standards that can be audited, Enforce & Measured  
• Threat Modeling ● Drills ● Secure by Design/Default/deployment |
| **Technology** | • Use a Next Generation Platform ● Automate actions  
• Security technology should collaborate ● Share IOC’s |
CYBER SECURITY MUST BE ON EVERYONE’S AGENDA

Executives
What is the potential impact of a cyber breach-attack
Mitigate Risk

Information Technology
We manage the IT Infrastructure & Software
We need to protect IT

Business
We need to use the Data
We need to use the Technology
We need to protect the DATA and Technology

ALL Employees & Contractors

CIO
Business Systems
Helpdesk
Data Centers
IT Security
IT Operations
Networks
Servers
Desktops

Operations
Marketing
HR
Legal
HSE
Supply Chain
Operational Technology
CYBER THREAT - ESSENTIALS

Information Sharing
- ONG-ISAC
- InfraGard
- Engage with FBI – DHS

Incident Response
- Invest on Preparedness
- Desktop exercise
- Root Cause Analysis

Executive Buy-In
- Everyone Responsible & Accountable
- Adopt the Safety Culture into Cyber-Security
- IT & OT need to work together

Build Cyber-Security Skill set
- Training
- Network with peers
- Adopt Best Practices

Concentrate in basic Cyber Hygiene
TAKEAWAYS

• Technology alone is not the solution
  • Information Sharing
  • Prepare for the worse

• Cyber-security is the responsibility of everyone

• Concentrate on Essentials & Cyber-security Hygiene

• Train your staff & build cyber-security skills
Questions?
USEFUL ORGANIZATIONS

• ONG-ISAC - http://www.ongisac.org/
• InfraGard – https://www.infragard.org/
• ISSA – http://www.issa.org/
• ISACA – https://www.isaca.org
• ICS-CERT
• US-CERT
• STOP-Think-Connect (http://www.dhs.gov/stophinkconnect)
• NIST - http://www.nist.gov/cyberframework/