

Louis & Associates

contact@l-a.lu

Cybersecurity :
From awareness to operations

14 April 2016

Awareness : Still a lot of work to do...

- Most of people think that they got those cool things for free just because some good angels want to pay for them



- And they don't realize how it infiltrates their privacy and what impacts it may have
- Don't realize that often times their devices are also an entry point to sensitive data/informations about the organizations they work for

Awareness : threats landscape

- **Foreign governments**
 - Mass surveillance
 - Spying on other countries
 - Support to their local economy
 - Criminal proactive prevention
 -
- **Cyber criminals**
 - Money extortion
 - Steal data (espionnage)
 - Hacktivism
 - Ruin people/organization's reputation
 - Fun
 -
- **Private Companies**
 - Commercial intelligence
 - Complying with regulations like Patriot Act
 -

Awareness : threats landscape : Governmental /privates organizations



UK gathering secret intelligence via covert NSA operation

Edward Snowden, "celui qui s'en est sorti"



MONDE | 29 décembre 2015 - 06h45

Edward Snowden incarne, lui, celui qui s'en est sorti **Edward Snowden** a révélé un mécanisme vieux de 15 ans : le sabotage de techniques de communication, transformées en

outils de surveillance **Edward Snowden** incarne cet idéal de partage des connaissances, fondé sur le développement individuel et

Lenovo caught yet again spying on Windows PC users

By [Chris Smith](#) on Sep 24, 2015 at 6:10 PM

COMPI

Meet Babar, a New Malware Almost Certainly Created by France

February 18, 2015 // 04:00 AM EST

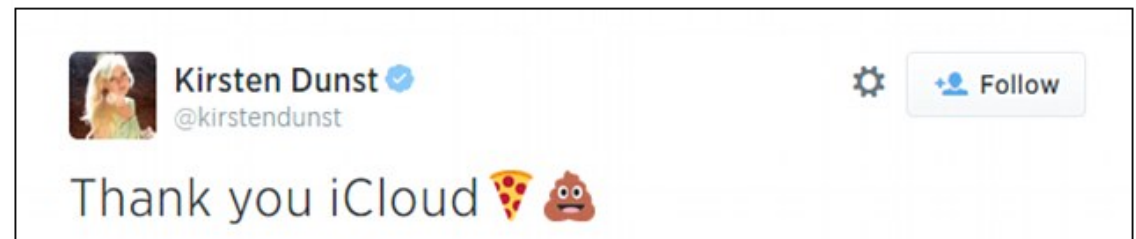
STUXNET: COMPUTER WORM OPENS NEW ERA OF WARFARE

Computer virus's evident success in damaging Iran's nuclear facility has officials asking if our own infrastructure is safe. Steve Kroft reports.



Awareness : threats landscape : Cyber criminal organizations

Kirsten Dunst has become the first celebrity to publicly criticize Apple after it emerged that a flaw in the 'Find My iPhone' function of its iCloud service may have helped a hacker to steal nude photos of her and '100 other celebrities'.



Panama Papers: biggest leak in history published by German newspaper

03/04 22:14 CET | updated at 04/04 - 19:42

Cyber crime

Warning issued: rise in ransomware crime in Luxembourg

Dropbox Confirms Compromised Account Details But Says Its Servers Weren't Hacked

Posted Oct 14, 2014 by [Natasha Lomas \(@riptari\)](#)

CNET > Security > 'Darkhotel' hack targets executives using hotel Internet

'Darkhotel' hack targets executives using hotel Internet

Using hotel Wi-Fi networks, the hackers are able to infect corporate executives' computers with malicious software, according to security research firm Kaspersky Lab.

Awareness : Other thoughts

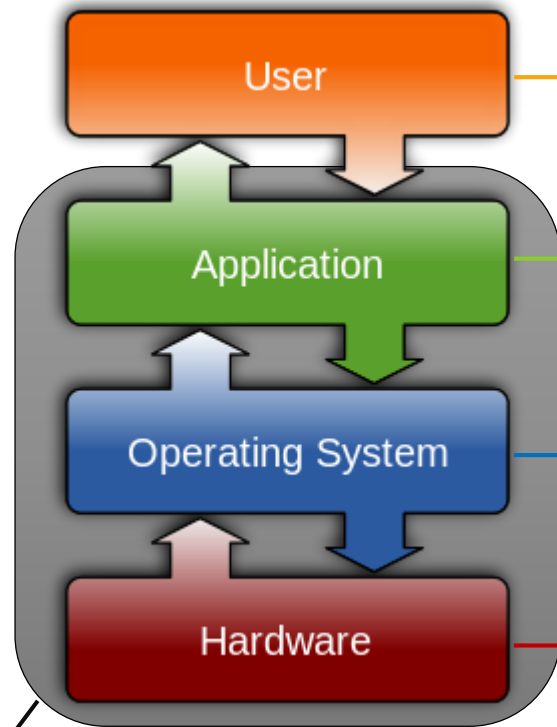
- Each US company must comply to the Patriot Act...
- Most of connected things are running US OS and SW
- Most of connected things are running on CN HW
- Connected things increase the attack surface and make data protection more difficult

« *Internet of things raises the question of internet of trust* »
(Stéphane LOUIS, Privacy and Cybersecurity consultant @ L&A)

Awareness : are we protected ?

- Computers scientists and IT security product editors/manufacturers make good job (**defense in depth**, next gen fw, Siem, Security framework, iso 27K etc ...)
- Is it enough when it comes to guarantying confidentiality of data ?
- What about protecting against ransomwares while keeping confidentiality of data ?
- We have smart AV and defense means but ... there are smart malwares and tricks...

Awareness : are we protected ?



- Sometimes careless, mistakes, ...
- Vulnerable to social engineering
- Where antiviruses fight against (known) malwares
- What about unknown/(too) smart malwares ?
- To what point can we trust it ?
- What about a malicious patch ?
- To what point can we trust it ?



















Computer / device / smartphone system perimeter

FW allows computer systems not to be directly exposed to danger but most of the time they are also US SW running on CN HW

Louis & Associates : who we are

- L&A, a Privacy Agency, was started in GD of Luxembourg in 2012 with the willingness to have liberty of movement without any pressure of any governmental or civilian institution
- L&A is specialized in security and Cyber Security, and uses its holistic view and expertise on those matters in order to enable efficient **privacy** and (highly) sensitive information/data protection of its customers
- Our team of headstrong, questioning and challenging veteran consultants from different horizons is our best asset to ensure a holistic view about securing your (highest) confidential information / data
 - Hackers (not crackers)
 - IT (security) specialist
 - Consultant with extensive experience in intelligence/counter intelligence

Louis & Associates : What we do

	Public & Private sector	Law enforcement & Military
Consultancy		
Privacy & Cybersecurity		
Privacy/Security Assesment		
Privacy/Security Audit		
Data Protection (Data leakage, ransomware,...)		
High sensitive data Protection (Espionnage, ...)		
Stealth communications (encrypted + no trace)		
Conference room spying bugs cleaning		
Big data computing on public information		
Offensive Cyber (strategy, design, setup, operations, ...)		

Operations : Challenges

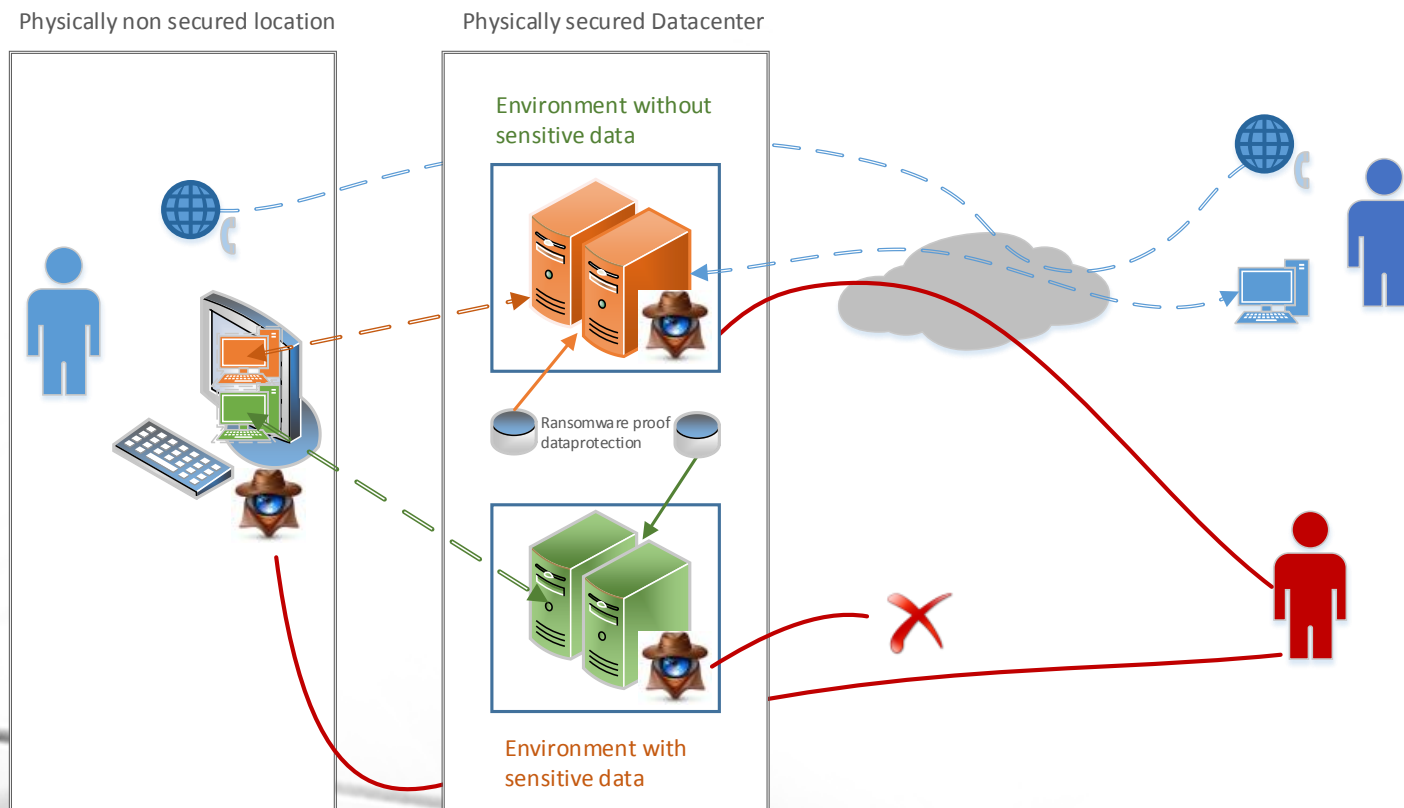
- Cybercriminality is a profitable growing business
- Standard counter measures are necessary but most of the time they protect against known threats
- Cybercriminal organizations have a lot of means and releasing new advanced malware every day...
- ... State of art of Cybersecurity includes being prepared to the unknown...

« Being prepared for the unknown implies always considering a system as being infected and living with that infection without getting damaged until it is detected and healed. »

(Stéphane LOUIS, Privacy and Cybersecurity consultant @ L&A)

Operations : L&A Approach

- When possible use a similar approach than in classified environment
 - Having an environment with low sensitive data
 - Another environment with sensitive data physically isolated from the previous one and internet also



- Smart Ransomware proof solution will allow to survive in case of successful ransomware attack
- Isolation prevents the undetected spyware to send away « sensitive informations » it has collected
- User into a non physically secured locations still vulnerable because his terminal can be tampered

Operations : L&A Approach

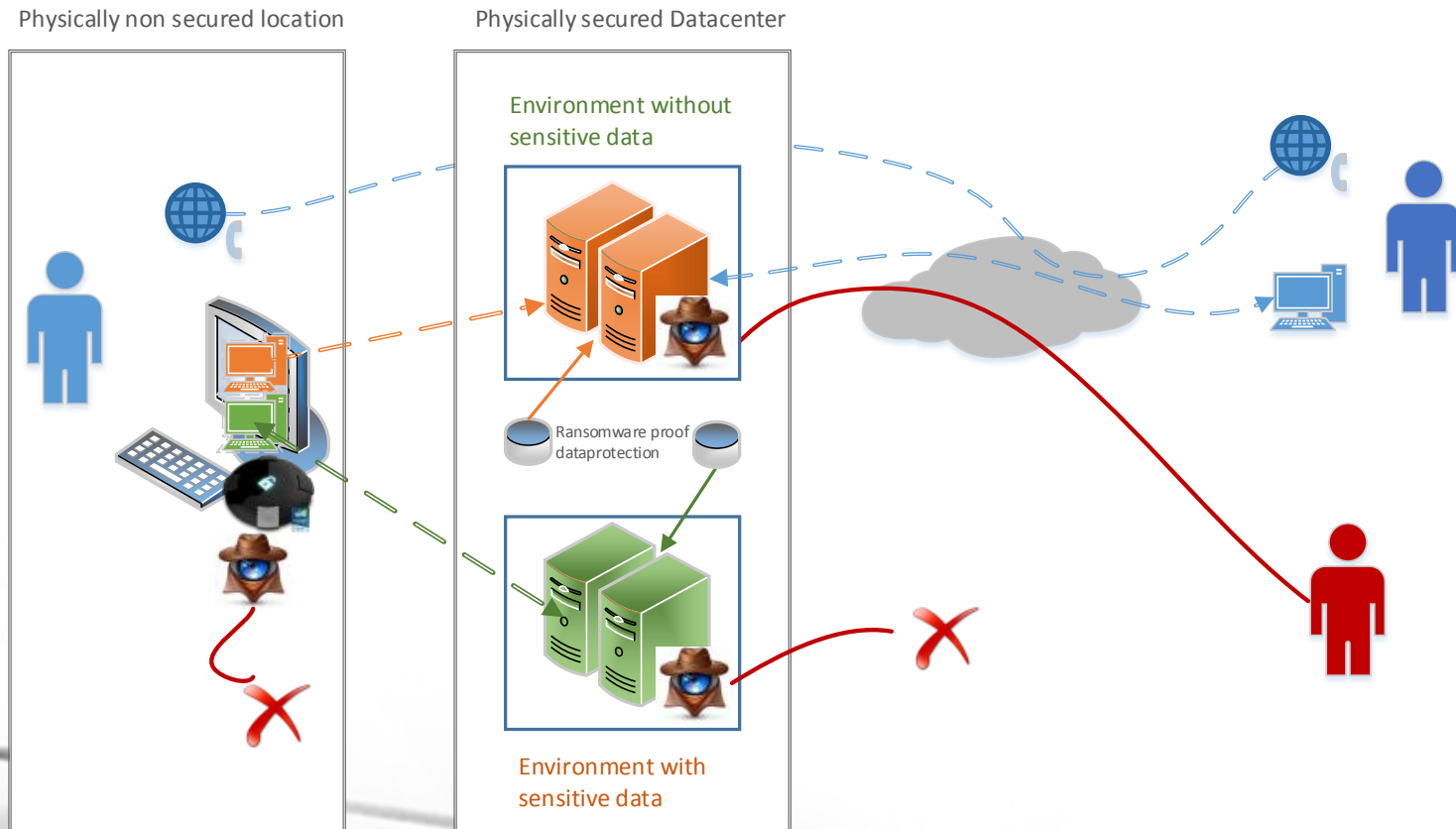
- Entry point of isolated environment must be done through **trustable** devices (at least at HW level, of course better if OS and SW can be trustable too)
- An entry point that may be sometimes unattended must be **tamper-proof**

*« Reducing attack surface remains a fundamental principle of cybersecurity but it must go along with the **reduction of surface of trust** at each entry point of the perimeter to be secured »*

(Stéphane LOUIS, Privacy and Cybersecurity consultant @ L&A)

Operations : L&A Approach

- Introducing a trusted tamper-proof computer that can be used as a terminal as well
 - Distribution
 - Retail
 - Integration



- Trusted tamper-proof computers/terminals allow any organization to deploy, in non physically trusted locations, end user devices that can be used as entry point sensitive/confidential data infrastructure and/or also manipulate sensitive/confidential data

Operations : Out of the box small smart solutions

- LuVOX
 - Stealth communications (encrypted + no footprint)
- LuSafe
 - Range of solutions to protect data against ransomware
 - Solutions so setup private/semi-private cloud storage ('private' dropbox like)

Cybersecurity from Awareness to Operations : Take Away

- TRUST is a key factor
- L&a
 - Hollistic view on Privacy, Security, Cybersecurity; securing (highly) confidential information from end to end
 - The best consulting services for top management
 - Active in Defence, EU and governmental institutions, Finance, and also SME concerned by privacy
- L&A approach for privacy protection
 - Designing security considering to be permanently infected
 - « *Defense in depth goes with defense in wide* » (S.Louis)
 - Reducing the surface of trust on the entry points to sensitive information/data
- L&A solutions out of the shelve for privacy (available for any integrator) protection
 - Exclusive distributor of elegant tamper proof computers
 - Solutions to setup private/semi-private cloud storage (dropbox like)
 - Stealth communications (email/phone)



**Take it
away**

« *You can trust L&A as your strategic partner to protect your highest confidential informations* »

tenki ขอบคุณคุณ takk спасибо kam sah hamnida
дзякуй hvala תודה dhanyavadagalu tack
gracias blagodaram mèsi xièxie tanemirt
arigatô manana diolch dziekuje bedankt rahmet enkosi mochchakkeram trugarez dank je
aciū grazzi ありがとう kia ora dankon dëkuji
tau barka शुक्रिया mamnun gràcie kaitos spas
teşekkür ederim bayarlalaa obrigada chnorakaloutiouin
sagolun murakoze taiku mahalo didi madioba chokrane rahmat
sukriya obrigado dakujem
terima kasih misaotra wela'in mercé najis tuke
asante grazie nandri 謝謝 mersi köszönöm sobodî اركش
mauruuru matondo cam on ban go raibh maith agat merci nanni vinaka
paldies ngiyabonga