Fail to Plan
Plan to Fail

A cautionary tale in incident response…

Don Reynolds
April 2016

Introduction

1

So what are the IR steps?

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

Focussing on Preparation.

The Obvious Stuff….

- People prepared
- Trained
- Maps of networks
- Locations and versions of types of software and systems
- Contacts for systems

Le "Baselining"

The Rob "M Lee" factor

- SANS ICS 515

What does "Normal" look like?

- Network packet captures
- Operating system dumps

Building Triage capabilities

- **Forget** standard IR response methodologies.

Le Contract

The definition of interactions with a supplier

- What does yours allow you to do?
- Needs to set expectations of what is to happen in exceptional circumstances.
- How will suppliers conduct themselves in delivery of a service?

Lets explore some exceptional circumstances…

Exceptional Circumstances

The right to cascade audit

- Third and fourth party outsourcing
- “Internal” outsourcing
- Assignment of obligations

The right to participate / conduct pentesting

The ability to conduct forensics / discovery

The ability to conduct IR investigations

Le Smoking Gun

Processor / Supplier will tell you if your data has been accessed. Really?

- Near Miss Notification?
- Deployment issues?

Unless it is proven that your data has been definitively compromised, there is no "smoking gun".

“Le Cloud” A.K.A. “Le Fog“

What is “data at rest”?

What is “processing”?

Why are there no security problems in the cloud?

Virtual Firewalls / VPN termination

Key Management / Container Management

CRH

Where exactly is *Le* Cloud?

Ireland.

Netherlands.

A little bit of Germany.

Philippines

China?

Ireland – A special place for hosting data

CERT

Digital Crime Division

Fraud Squad

Personal Data vs IPR & Copyright

Office of the Data Protection Commissioner – Enforcement

Examples that made it into the news

Its not just Ireland……

“So you must be Ze Cloud Hater?”

Not really….

Its not just me expressing reservations about cloud provision models.

Lack of transparency is critical. Hype is not a protective shield for my organisation’s data.

Dr Giles Hogben - ENISA

Somebody else's problem (SEP) syndrome

"*Appirio Cloud Storage fully encrypts each piece of data as it passes from your computer to the Amazon S3 store. Once there, it is protected by the same strong security mechanisms that protect thousands of customers using Amazon's services*" (Thanks to Craig Balding, cloudsecurity.org for spotting this)

Dr Giles Hogben - ENISA

Amazon AWS ToS

- "YOU ARE SOLELY RESPONSIBLE FOR APPLYING APPROPRIATE SECURITY MEASURES TO YOUR DATA, INCLUDING ENCRYPTING SENSITIVE DATA."

- *"You are personally responsible for all Applications running on and traffic originating from the instances you initiate within Amazon EC2. As such, you should protect your authentication keys and security credentials. Actions taken using your credentials shall be deemed to be actions taken by you."*

Dr Giles Hogben - ENISA

Compliance Challenges

- Cloud Provider cannot provide evidence of their own compliance to the relevant requirements.
- Cloud Provider does not permit audit by the Cloud Customer.
- In certain cases, using a cloud implies certain kind of compliance cannot be achieved

Colours of the clouds…..

Black Cloud

Software as a Service

Grey Cloud

Can audit to the Hypervisor

White Cloud

Auditable to the Metal

Legislation Curveballs for IR

Where are you located?

Where are the people whose data is being processed?

Where is the data being stored?

Where is the data being shared with?

- **Labour Law.**
- **Data Protection Law of personal Information.**
- **Monitoring of individuals in the workplace.**

Safe(?) Harbor is Dead….

Max Schrem is my hero…

What comes next?

Fin

(The End)