A Trusted Supplier Counts

Presented by Konstantinos Panagos
Sep 23, 2013
Athens

Agenda

- 1. A word about Integrity
- 2. Our role as a Supplier and a Purchaser
- 3. What our customers want and what other stakeholders think of ?
- 4. What tools we have to protect ourselves and our customers data?
- 5. It happened ?
- 6. What we need from the Supply Chain? Working together.

1. Integrity : It’s all Greek to me

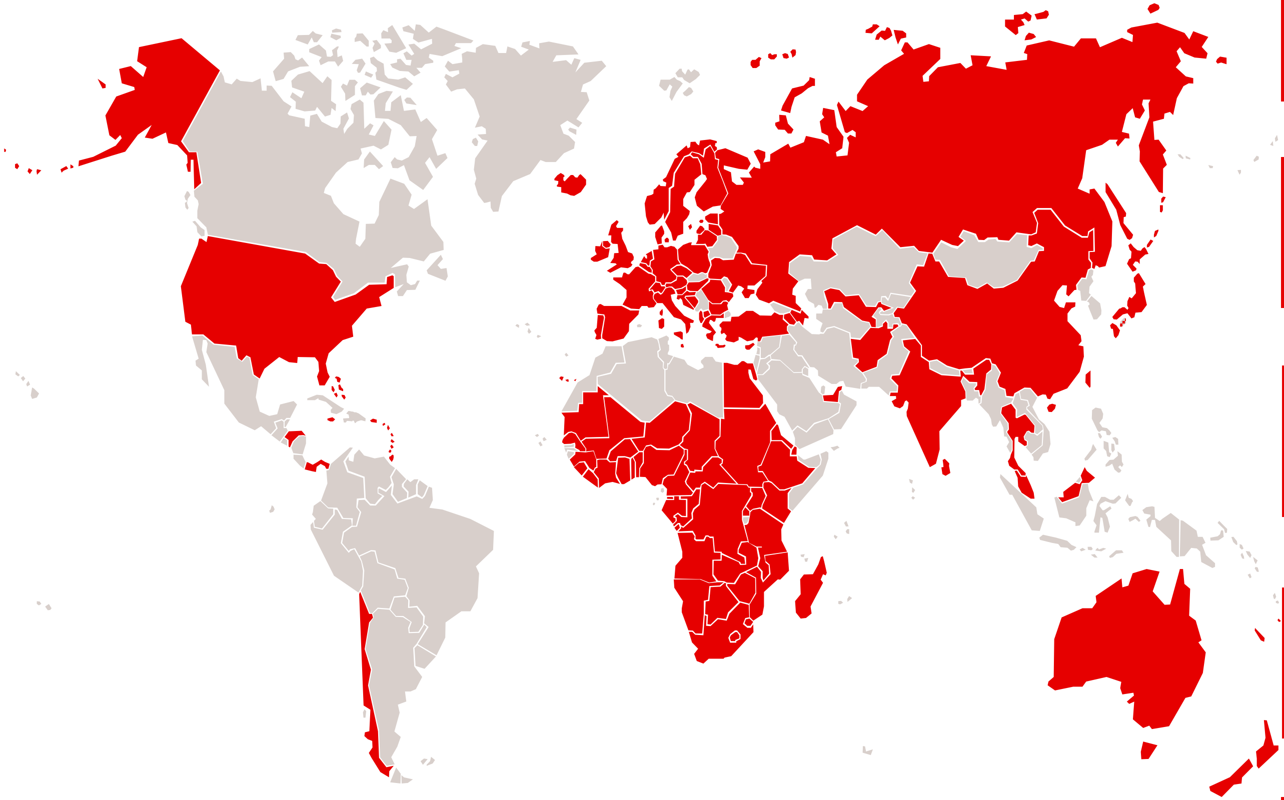
Integrity -> integer -> A-ΚΕΡΑΙΟΣ -> A-ΚΕΡΑΙΟΤΗΤΑ

A : for non existent , not wanted

- Greek language uses three different words for “mix”
- "φύρομαι" = mix liquid and solid (e.g. "αιμόφυρτος").
- "μίγνυμι" = mix of solids (e.g. "μίγμα").
- **ΚΕΡΑ-**ΝΥΜΜΙ : for mix liquids “κέρασμα, kerasma”

- So, Integrity is about the **non existence of unwanted materials,** in our case **in our whole supply chain**.

2. Our role as a supplier and a Purchaser Vodafone's global presence…



Today, 1 in 5 mobiles are connected to the Vodafone network

49Bn+ security events tracked in June2013

60M+ viruses cleaned and removed yearly

1M MMS malware threats removed monthly

2.6M "intrusion" attempts blocked in May 2013

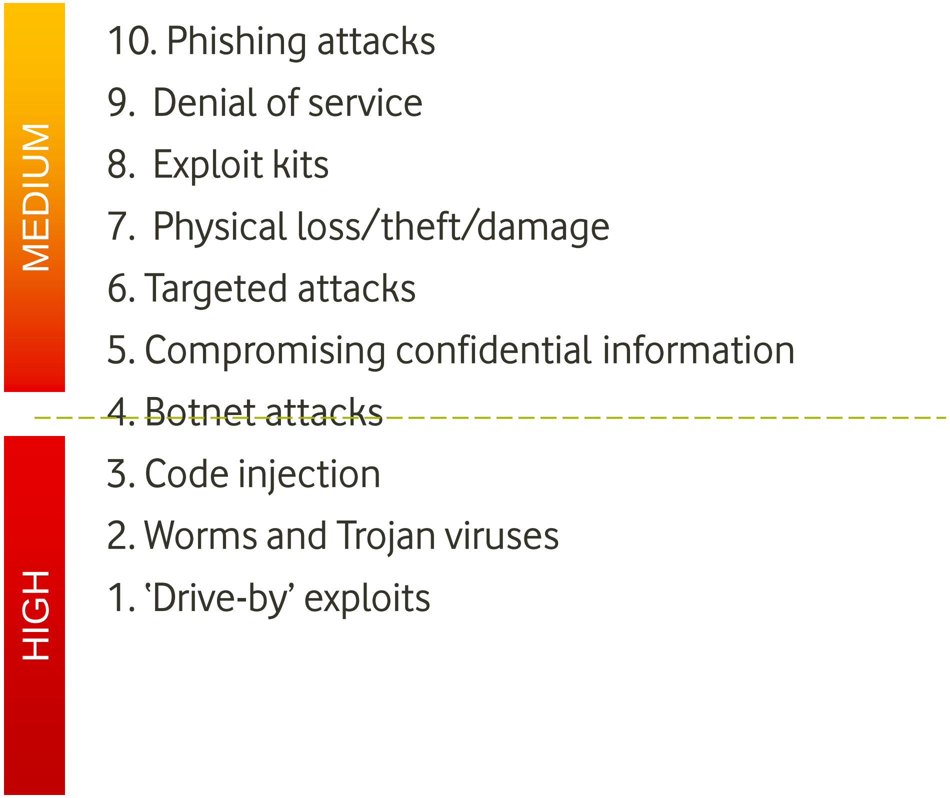
6 Denial of Service attacks globally in H1 2013

faces many threats…

It is predicted that by 2016 use of the mobile internet will exceed that of the wired internet

Source: IDC WW Intelligent Systems: 2011-2015

ENISA Top Mobile Security Threats



10. Phishing attacks
9. Denial of service
8. Exploit kits
7. Physical loss/theft/damage
6. Targeted attacks
5. Compromising confidential information
4. Botnet attacks
3. Code injection
2. Worms and Trojan viruses
1. 'Drive-by' exploits

3. Privacy and security concerns

- **Confidentiality of their personal and private communications** – a basic issue for a communications company
- **Collection of their personal information** – mobile operators have access to a lot of sensitive information including customers' personal communications, their location and how they use the internet
- **Security of their personal information** – the complexity of technology, threats from hackers and the potential for human error can lead to information being lost or deleted or getting into the wrong hands
- **Use of their personal information** – as more services use mobile data for advertising and analytics, customers need to be able to control how information is used and provide consent
- **Additional privacy issues from smart phones, apps and new technologies** (such as connected cars, smart grids and mHealth) – for example, mHealth services may mean that patient health records are transmitted across mobile networks and individual apps often require their own privacy permissions to collect and use data

Stakeholder views

"Vodafone will have to ensure that users can use your networks with confidence, that you are protecting their privacy. To do so, you will have to compel action amongst device manufacturers, operating system developers, and other parties to ensure that privacy is protected across the layers."

Gus Hosein, Executive Director, Privacy International

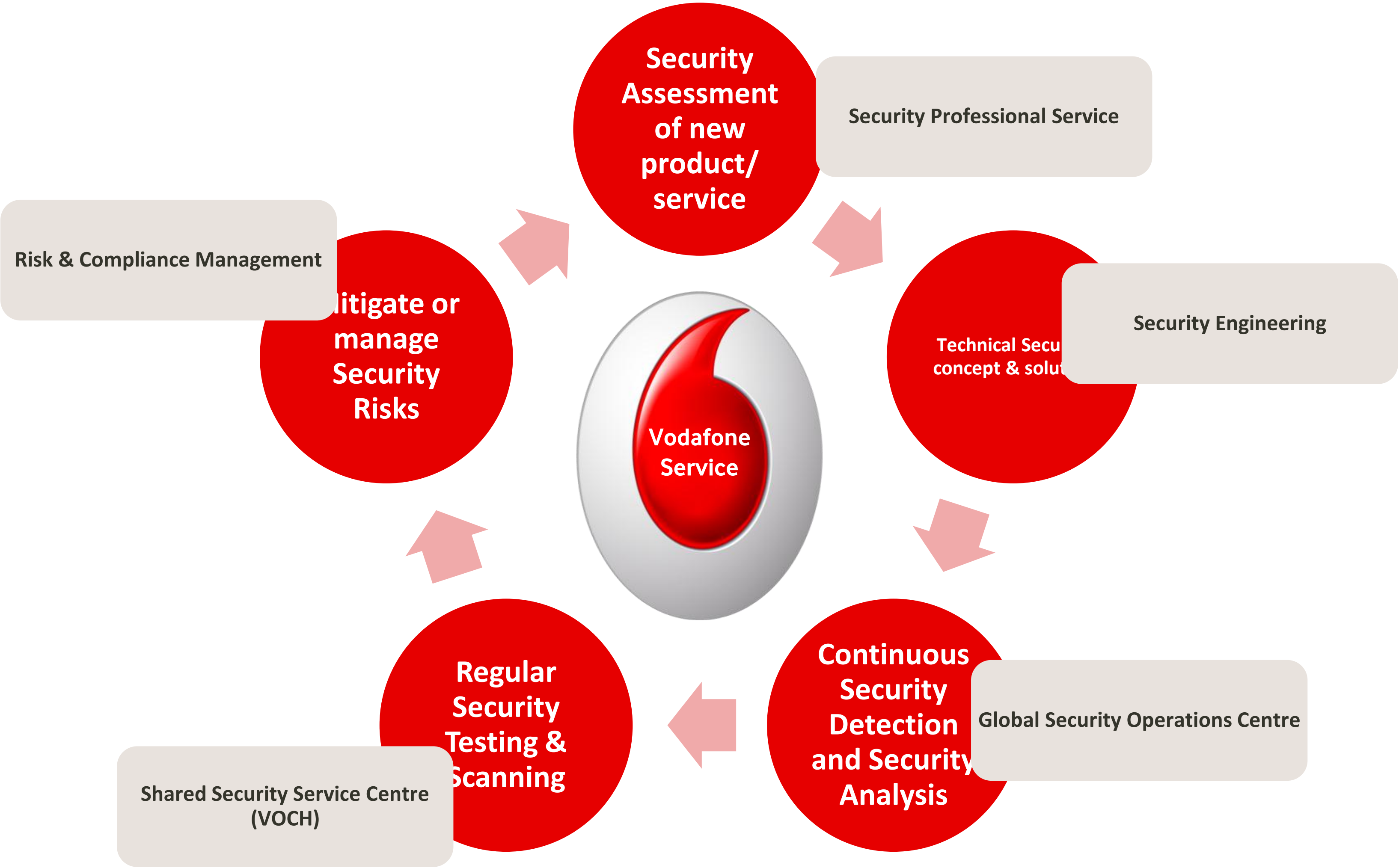
4.How Vodafone acts on Privacy and Security

Our Safeguards linked to the Supply Chain :

Certificate No:362212/F

- Our Risk Management System ensures among others,
- **Supplier review** – Process to review suppliers, such as outsourced call centres and companies that provide hosting platforms or manage customer data, and ensure measures are in place
- **Product and service review** – Processes for taking privacy into account when developing products and services (such as privacy-by-design in mobile applications)
- **Incident management** – Process for managing incidents, such as data security incidents and losses of data
- **Disclosure** – Processes for governing all disclosures of personal information, such as in response to legally mandated government requests and assisting law enforcement authorities
- **Data management and retention** – Processes for managing the lifecycle of data, including destruction and retention of data
- Our core data centres in Germany, India, Ireland and Italy are **certified to ISO 27001. VF-GR certified since 1999.**
- We require our **external suppliers and partners** to **meet defined minimum security standards**, and
- We conduct **risk assessments and due diligence exercises** to provide assurance that these are being met in practice**.**

4. Tools to protect ourselves and our customers.
We take a lifecycle approach to Technology Security



Security Assessment of new product/ service

Security Professional Service

Technical Secu concept & solut

Security Engineering

Continuous Security Detection and Security Analysis

Global Security Operations Centre

Regular Security Testing & Scanning

Shared Security Service Centre (VOCH)

litigate or manage Security Risks

Risk & Compliance Management

Vodafone Service

…built on a consolidated, effective Technology Security strategy.

3 key areas for success:

1 **Focus on threat, visibility and control** through provision of centralised security services

2 **Technology transformation** to deliver security through truly flexible solutions

3 **Innovative security applications** to help Vodafone to stay ahead of the game

- **Security in the culture of the organisation**
- **Mitigate a global risk profile**
- **Utilise best in breed security solutions**
- **Deliver a consistent security portfolio**

Centered on a Security Centre of Excellence…

Focus On THREAT, Visibility & Control

- Centralised service and control
- Security made simple
- Global service
- Consistent security portfolio
- Reduce the threat profile

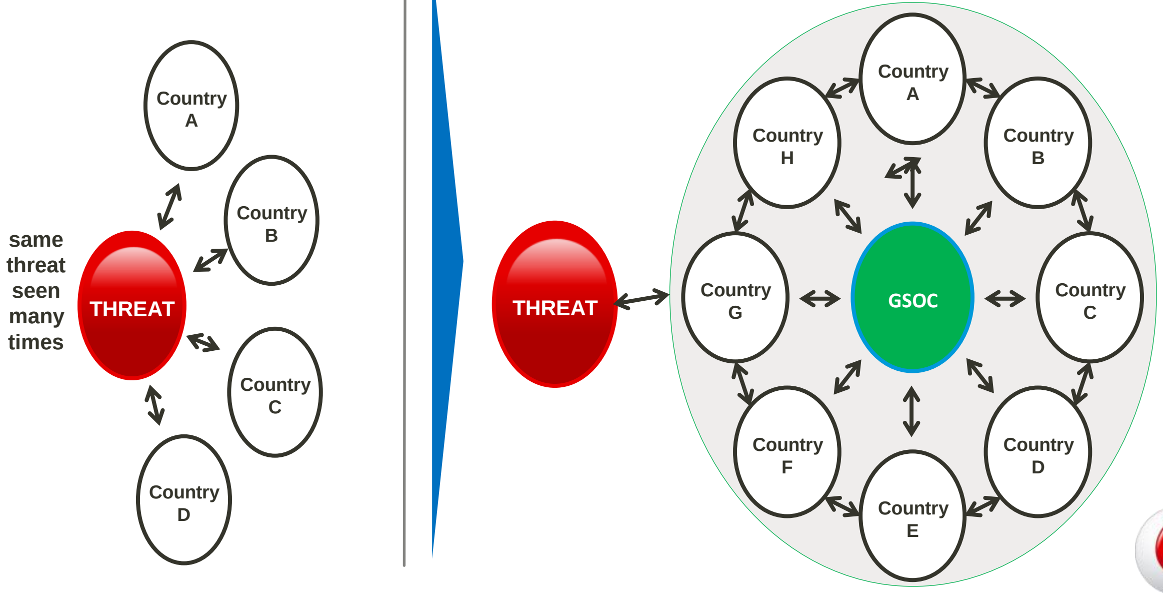
The Challenges

- Visibility and control of international threats
- Simplification & transparency
- Globally consistent services, support and threat management

The Solution

Before
Security managed locally

Today
Globally Secure perimeter
Central management - localised controls



5. It happened ? **Spear phishing compromises two company networks**

Industry: Financial

Incident: Spear phishing attack used against a smaller, less secure financial institution in order to gain access to a larger one through trusted access. Spear phishing targets specific individuals who can provide inadvertant access to very specific devices or data.

Why it happened: Hackers took advantage of social networking and known PDF exploits in order to plant malware on the targeted user's machine. This was accomplished by conducting a social engineering campaign against the specific target. Over time, the attacker was able to learn the victim's position within the company, office location and work schedule.

Eventually the attacker knew enough about the victim to create a spear phishing message that would not be viewed as suspicious. Once the victim opened the attached malicious PDF, the attacker gained access to the user's workstation and the user's network as well as the network of the company's larger partner. Once a foothold was gained, covert communication channels were established for use in sneaking data out of the company's networks.

Damage done: Both financial institutions had personal information about their clients stolen.

Lessons learned: The lessons learned in disrupting and remediating this situation led to the development of new policies and guidelines—including new correlation rules and approaches to anomaly detection—that could be used to block this type of incident in the future.

Source : IBM June 2013 IBM Security Services Cyber Security Intelligence Index June 2013.

It happened ? **Voice Mail Hacking**

- **Phone-hacking scandal:**
- The extent of phone hacking at the News of the World led to the closure of the paper after 168 years. Allegations of phone hacking first emerged in 2005 and eight people, including two former editors of the News of the World, have now been charged with conspiring to intercept voicemails. The charges relate to 600 alleged victims, including celebrities, sport stars, politicians and victims of crime.
- **2005 Origins of the scandal**
- In November, the newspaper's royal editor, Clive Goodman, writes a story about Prince William suffering a knee injury. Buckingham Palace suspects the prince's voicemail was hacked to get the story and in December calls in Scotland Yard. In August 2006, police arrest Goodman and private investigator Glenn Mulcaire for illegal phone hacking
- **HOW**: Standard password in the Voice mail Service, then a common feature .
- Source : http://www.bbc.co.uk/news/uk-14124020

NEWS OF THE WORLD
Edition number 8,674
The world's greatest newspaper 1843-2011
FERGIE SELLS ANDY FOR £500K
THANK YOU & GOODBYE
After 168 years, we finally say a sad but very proud farewell to our 7.5m loyal readers
INSIDE: 48-PAGE SOUVENIR PULLOUT
PROFITS FROM THIS HISTORIC EDITION WILL GO TO CHARITY
JACKO'S DEATHBED

6. Working together :Role and expectations from supplier

- Understanding of local situation/needs aside Global scope and size.
- Respect and design for local Regulatory requirements: One size does not fit all.
- Security updates : immediate response , not waiting for global releases to fix holes.
- Customer view : see end customer not the operator, end user not interested in next global release.
- Don’t focus only on the obvious or large contracts – small ones can be costly too…
- “Follow the information”
- Standardisation , ISO 27036 will assist making it easier for the whole supply chain.

6. Working Together. Securing Information in the Supply Chain

- Understand and respect that we need to identify all information shared with suppliers
  - Information led – not supplier focused !
- Quantify the risk to determine a proportionate response
  - Identify the information that constitutes an unacceptable business impact if breached
- Costs
  - Identify resources that can be focused with minimal impact
  - Leaking of sensitive material e.g. config docs, customer info may cause sanctions
  - Purchaser must be given FULL support during investigations e.g. logs etc.
- Disruption to existing relationships ?
  - Fit in with existing procurement and vendor management processes.
  - Consistent approach.

6. Working Together . Final words

- Auditability and Code Traceability with independent review where necessary
  - No unsupported third party software should exist
  - Architectural design – compare the control vs. designed version
  - Architectural deployment – compare the control vs. the deployed version

- All "features" must be declared even if not for operator use or unlicensed
  - Secure and (cryptographically) authenticated operator controlled debug and maintenance
  - Role based access controls !!

- Penetration and robustness testing must take place
- Secure at rest all sensitive data
- Terminals : The gate to our networks , equal attention as any fancy Core Network Node.

Thank You

Presented by Konstantinos Panagos
Sep 23, 2013
Athens