



LA NOSTRA ESPERIENZA CON WANNACRY

L'EVOLUZIONE DELLA DATA PROTECTION

*Elisa Garavaglia – Chief Security Officer
Responsabile Security e IT Governance, Quixa*

CYBERTECH PRACTICAL WORKSHOP
“MALWARE E CYBER CRIME PREVENTION”

Milano, 26 ottobre 2017

Agenda

- Chi siamo e come siamo organizzati
- L'esperienza WannaCry
- Il programma di *Data Leakage Prevention*



Chi siamo



Un ottimo valore per un ottimo prezzo!



Un acquisto intelligente: risparmiare denaro senza perdere qualità!



Il giusto mix tra un'assicurazione tradizionale e una diretta!

Il brand principale dedicato ai **clienti diretti**



*Only for prospects with a saved quotation

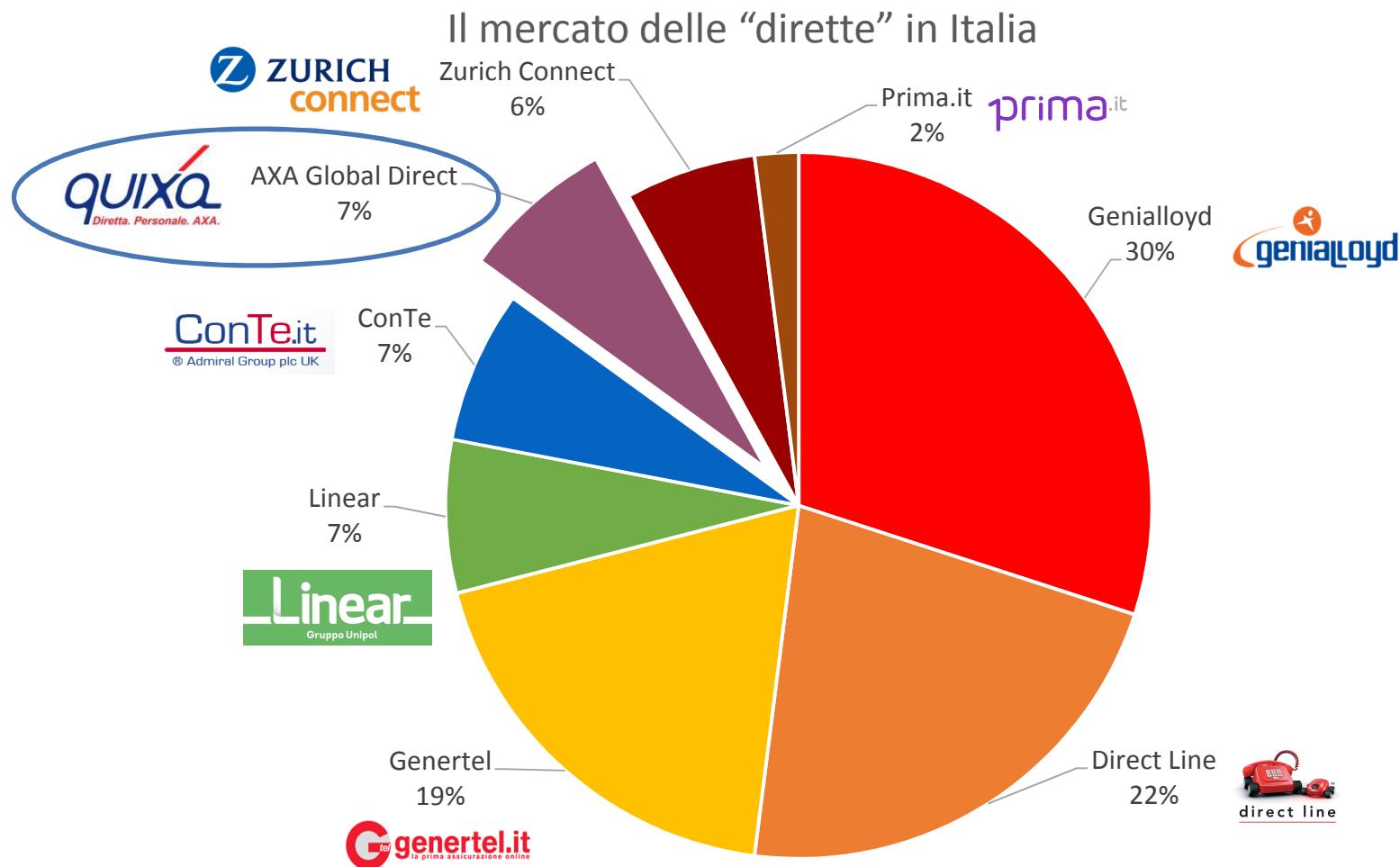
Il secondo brand per competere negli aggregatori e spingere sui servizi fai da te (per i **clienti diretti più smart**)



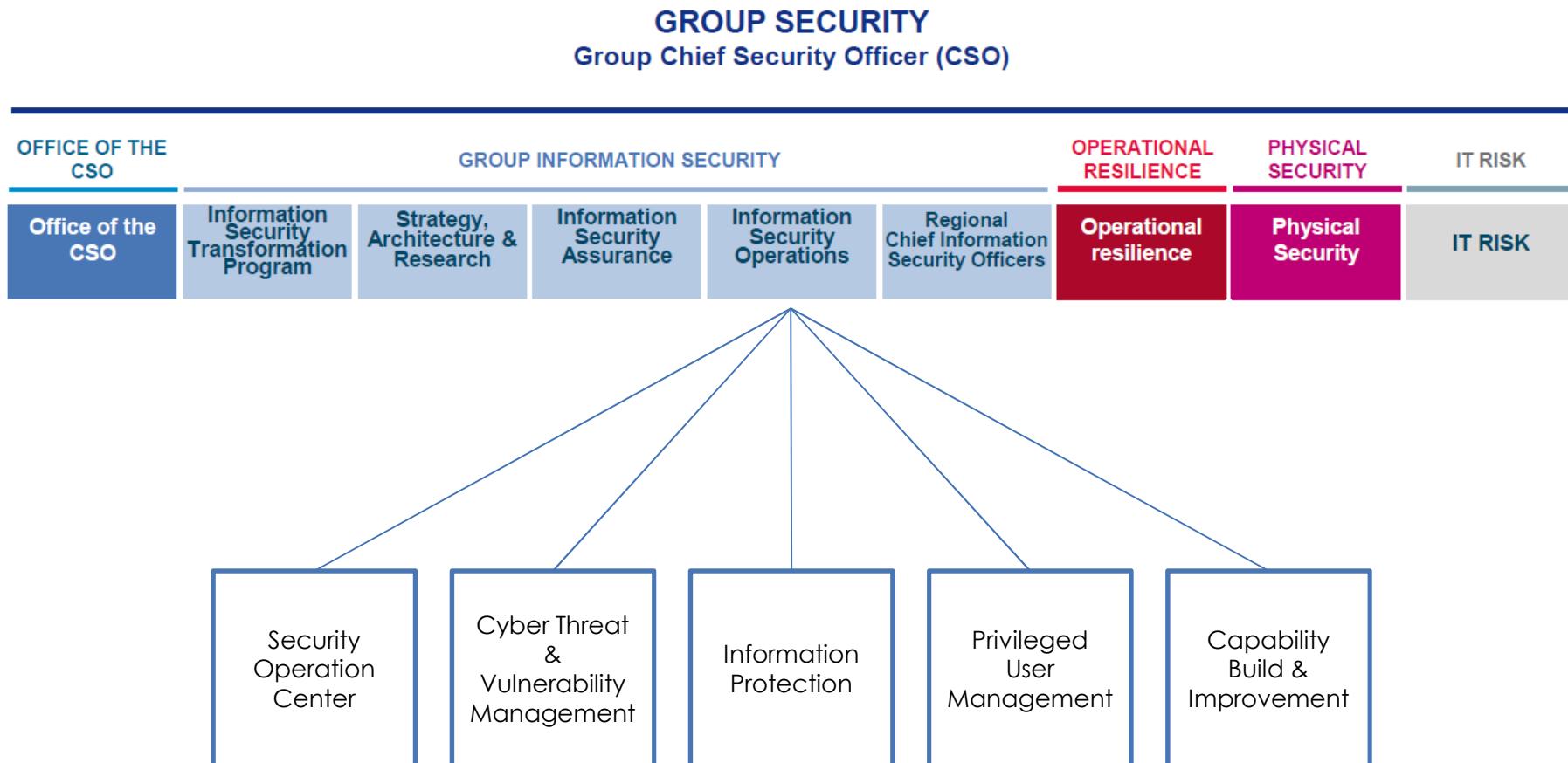
Vendite nelle agenzie (per i **clienti ibridi**)



Il mercato “diretto” in Italia

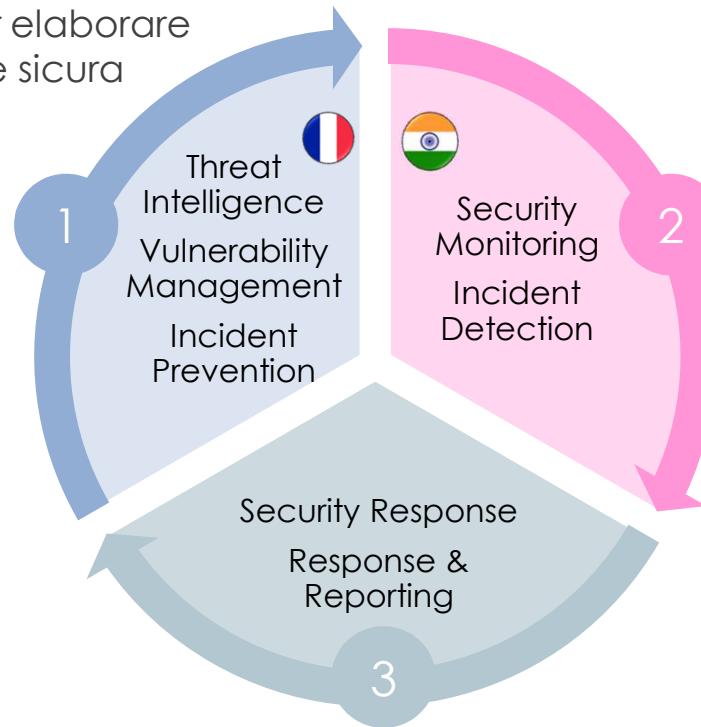


AXA Group Information Security - organizzazione





- Analisi di *threat intelligence*
- Report accurati e aggiornati sulle vulnerabilità
- Correlazione di rischi per elaborare una risposta adeguata e sicura



- 24/7 monitoraggio *real time*:
 - Firewalls & WAF
 - Access Management
 - Intrusion Prevention
 - DDOS
 - AV e Endpoint
 - Infrastruttura dei Server
 - Applicazioni
 - Middleware

- Correlazione di eventi mediante analisi accurate e *business-driven*
- Risposta agli incidenti rapida ed efficace grazie a un coordinamento centralizzato
- Analisi dettagliata e investigazioni forensi avanzate

L'Esperienza Wanna Cry



L'esperienza WannaCry 1/2

prima di maggio
2017



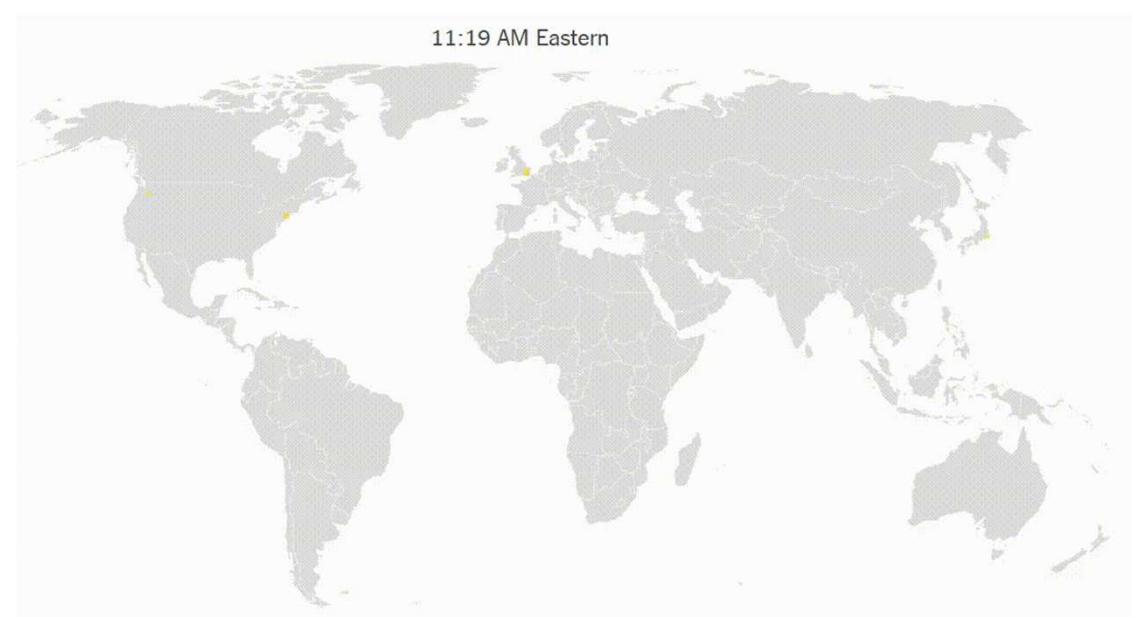
I gruppi di ricerca MalwareHunterTeam, GData e Malwarebytes hanno osservato il malware Trojan.Encoder.11432 (conosciuto anche come WannaCry) alcune settimane prima dell'attacco, ma senza rilevare una distribuzione tale da far pensare ad un attacco imminente.

12 maggio
2017



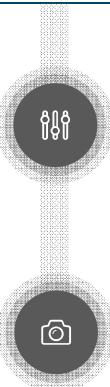
Inizia l'attacco

Venerdì 12 maggio è iniziato l'attacco, con i primi segnali registrati nella mattinata quando Telefonica (il noto ISP spagnolo) dirama un avviso in cui chiede raccomanda ai propri clienti di spegnere i computer per via di un attacco informatico in corso. In poche ore il *ransomware* inizia a mietere vittime in tutto il mondo.



L'esperienza WannaCry 2/2

13 maggio
2017



Parte l'*alert* dalla Security spagnola

Il CISO spagnolo ci contatta a proposito delle piattaforme condivise gestite in Spagna: vengono identificati i server che potrebbero essere stati impattati.

13-29 maggio
2017



Iniziano le azioni di contrasto

Avviene l'ingaggio da parte del Portogallo: comincia il patching dei server. A livello locale partono varie attività sulla workstation e sulla NAS.

AXATECH - WannaCry Ransomware Security Warning

External Security Threat – Prevention Warning – High Alert

What is happening?

Major companies worldwide are experiencing ransomware attacks since last Friday. A ransomware threat known as WannaCrypt0r/WannaCry has affected Windows computers in at least 99 countries worldwide, impacting 230.000 computers. The attack has been described by Europol as unprecedented in scale.

What you should do?

Currently no cases have been reported on AXA Information Systems, but, as a prevention measure until further notice:

- Do not click on URLs in emails.
- Do not open any attachments which are not business critical and not from a known source from outside of AXA
- Do not access your personal e-mail (Gmail, Yahoo etc.) using your AXA device.

If you see something suspicious or the WannaCry Ransomware notice screen, informing you that your files have been encrypted?

If you see something suspicious or your computer has been infected, (it will display a notice screen), please shut it down immediately and call the AXA IT helpdesk in order to log the incident or local security team.

IT Helpdesk phone number:

IT helpdesk email:

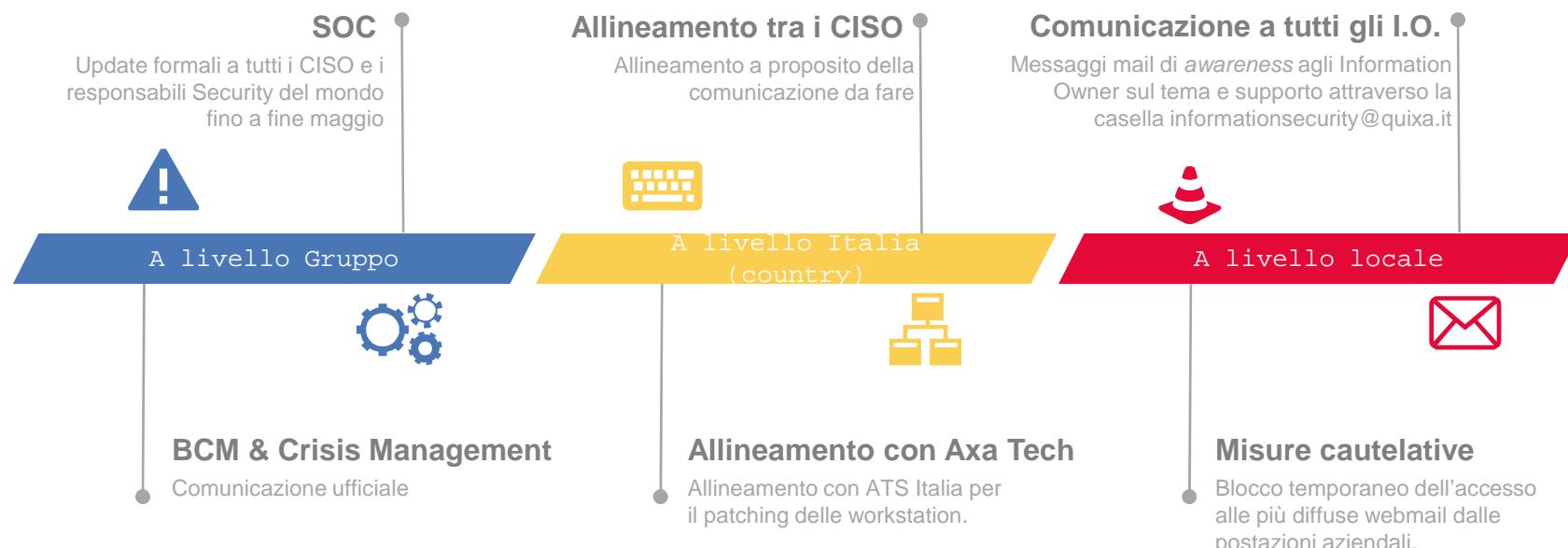
Local Information Security phone number:

Local Information Security email:

Thank you for your vigilance and support, and your IT and Information Security teams will remain on High Alert until further notice.

OK

Cosa è stato fatto ai diversi livelli



Next step: data
protection



Data Protection



Rischio globale

Il Data Leakage è stato identificato da AXA come "rischio globale".

Il Group Security ha definito le linee guida per il DLP, identificando vari obiettivi da raggiungere per mettere in sicurezza la compagnia.

Report trimestrale

Il piano prevede raccomandazioni a breve/medio termine che devono essere rendicontate al Gruppo con cadenza trimestrale.

Obiettivi suddivisi per livelli

A tutte le Compagnie è richiesto il raggiungimento di alcuni obiettivi BASE mentre gli obiettivi AVANZATI sono richiesti o meno in base all'esposizione della Compagnia al *Cyber Risk* (valutazione effettuata dal *Risk Committee*).

Identificazione di priorità

Tra le principali azioni identificate come fondamentali ci sono:

- Classificazione dei dati
- Identificazione dei *Crown Jewels*
- External network protection
- Email & Cloud protection
- Mobile device protection

Data Protection – Tactical Plan 2017

Obiettivo: non solo ridurre il rischio di sottrazione/diffusione illecita di informazioni aziendali ma anche proteggersi dalla diffusione di malware



SITI WEB FILE SHARING



WEBMAIL GMAIL, YAHOO, ...



HARDWARE PORTE USB E SUPPORTI ESTERNI

