Diamo energia al Sistema con tecnologia e informatica

Un punto di forza per il Sistema.

BCC CREDITO COOPERATIVO

BCC Sistemi Informatici

“ Il ruolo del CISO (Chief Information Security Officer) in una realtà bancaria Complessa ”

«Security Summit 2016»

“Lorenzo Possenti”

Milano, 17 marzo 2016

AGENDA

- La Società
- Le responsabilità del CISO
- Business Continuity
- La sicurezza in Banca
- L'analisi del rischio informatico
- Cyber security

"Lorenzo Possenti"

Milano, 17 marzo 2016

LA SOCIETA'

«Security Summit 2016»

"Lorenzo Possenti"

Milano, 17 marzo 2016

LA SOCIETA'

BCCSI è uno dei maggiori outsourcer informatici del Credito Cooperativo ed è parte integrante del Gruppo Bancario ICCREA; nel 2014 ha effettuato la convergenza ed integrazione dei sistemi (Switch Over) attraverso il progetto di consolidamento dell'infrastruttura informatica a livello nazionale, con l'accentramento dei rispettivi Data Center su un'unica piattaforma hardware:

- eroga il sistema informatico ed informativo a circa 140 BCC Clienti con circa 18000 client totali;
- eroga il servizio di Home Banking denominato Relax Banking con circa 900.000 utenti (end user);
- con un fatturato di circa 84 milioni di euro.

LE RESPONSABILITA' DEL C.I.S.O.

«Security Summit 2016»

"Lorenzo Possenti"

Milano, 17 marzo 2016

LE RESPONSABILITA' DEL CISO IN BCCSI

In BCC Sistemi Informatici del Gruppo Bancario Iccrea, ricopro il ruolo di Responsabile della Sicurezza con delega sulla Business Continuity; mi occupo in particolare di:

- coordinare tutte le attività inerenti la Continuità Operativa e il Disaster Recovery;
- predisporre ordini di servizio e circolari sulla Sicurezza e Continuità Operativa;
- definire e aggiornare le policy di sicurezza;
- aggiornare la documentazione (Sicurezza, Continuità Operativa, Disaster Recovery, analisi dei rischi informatici) anche in merito alla compliance;
- coordinare il Change Advisor Board – CAB per le change infrastrutturali rilevanti;
- gestire e tracciare gli incidenti di sicurezza informatica;
- coordinare il processo di comunicazione con i 140 security manager delle Banche Clienti;
- partecipare allo svolgimento dei test di sicurezza prima dell'avvio in produzione di un sistema nuovo (es. token home banking);
- definire gli amministratori di sistema in risposta ad uno specifico provvedimento del Garante della Privacy;
- coordinare le attività di penetration test, vulnerability assessment e remediation plan.

BUSINESS CONTINUITY

&

DISASTER RECOVERY

«Security Summit 2016»

"Lorenzo Possenti"

Milano, 17 marzo 2016

BUSINESS CONTINUITY

BANCA D'ITALIA

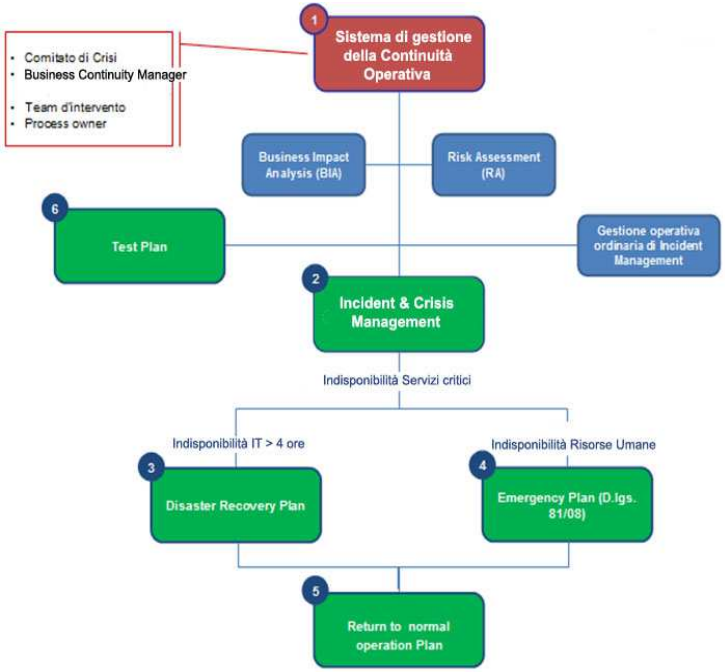
- Disposizioni di vigilanza per le Banche («Circ. 285 di Banca D'Italia - TITOLO IV – Capitolo 5 La Continuità»);

BUSINESS CONTINUITY PLAN

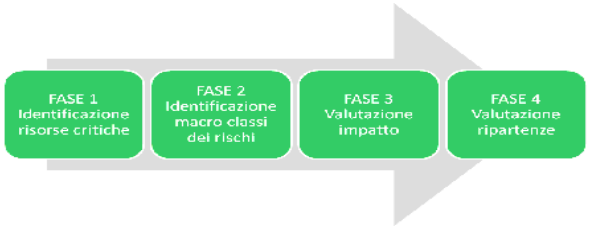
- Il Piano di Continuità Operativa di BCC Sistemi Informatici è conforme alla norma internazionale ISO 22301;

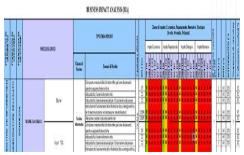
SCENARI DI RISCHIO E BIA

1) Distruzione o inaccessibilità di strutture nelle quali sono allocate unità operative o apparecchiature critiche;
2) Indisponibilità di sistemi informativi critici;
3) Indisponibilità di personale essenziale per il funzionamento dei processi aziendali;
4) Interruzione del funzionamento delle infrastrutture (tra cui energia elettrica, reti di telecomunicazione, reti interbancarie, mercati finanziari);
5) Alterazione o perdita di dati e documenti critici.



TEST ANNUALI





DISASTER RECOVERY

❑ DISASTER RECOVERY

- ➢ Recovery Point Object – RPO
- ➢ Recovery Time Object – RTO.

❑ SCENARIO E OBIETTIVO DELL'ULTIMO TEST

- ➢ Il test ha raggiunto l'obiettivo di erogare l'operatività ordinaria di Banca aperta alla propria clientela con la partecipazione di 21 Banche/Società (19 Banche Clienti, 1 centro servizi, 1 Federazione) e 171 risorse impegnate.

LA SICUREZZA IN BANCA

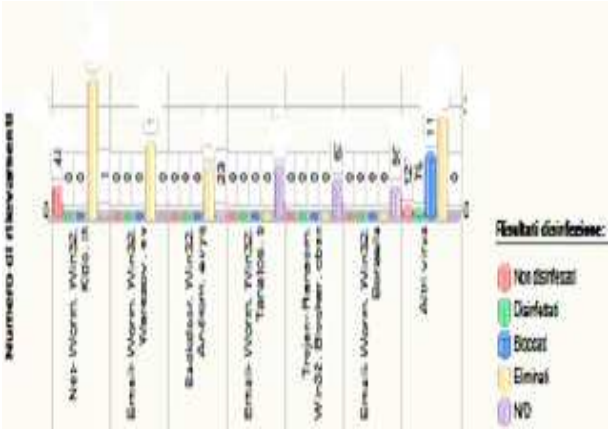
«Security Summit 2016»

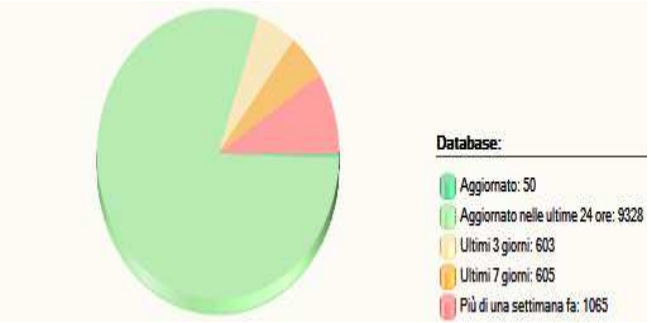
"Lorenzo Possenti"

Milano, 17 marzo 2016

LA SICUREZZA IN BANCA

- **ACCESSO IN MPLS (Multi Protocol Label Switching)**
  - Segregazione del traffico dati/voce attraverso VRF (VPN Routing and Forwarding);
  - ogni Sede con le rispettive filiali, ha la propria VRF;
  - sulle VRF vengono applicati dei filtri sui Firewall generati secondo le policy aziendali.
- **POSTAZIONE DI LAVORO**
  - accesso alla macchina tramite credenziali NON amministrative;
  - antivirus a bordo con signature aggiornate;
  - utenza con tempistica di scadenza password inferiore rispetto ai valori minimi di sicurezza;
  - posto di lavoro integrato nel dominio proprietario della Banca;
  - connessione indiretta verso Internet pilotata tramite proxy, firewall, web filtering;
  - accesso al sistema informativo tramite BCC Security composto da SDBMAN e WPROF.





LA SICUREZZA IN BANCA

❑ RELAX BANKING

Relax Banking, nelle versioni Famiglia o Impresa, permette di eseguire le principali operazioni bancarie in sicurezza grazie al dispositivo OTP (token fisico) che genera password monouso:

- Circa 900.000 Clienti;
- accesso in strong authentication;
- accesso anche da smartphone e tablet con app dedicate;
- protocollo con chiave di cifratura a 128 bit.

L'ANALISI DEL RISCHIO INFORMATICO

«Security Summit 2016»

"Lorenzo Possenti"

Milano, 17 marzo 2016

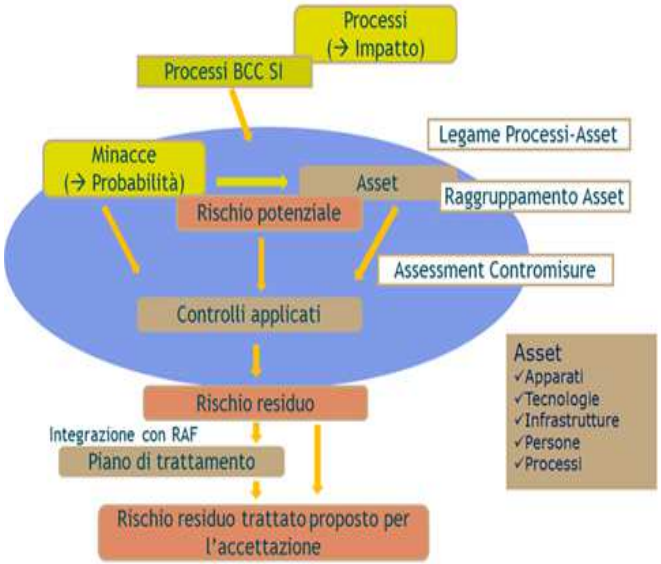
L'ANALISI DEL RISCHIO INFORMATICO

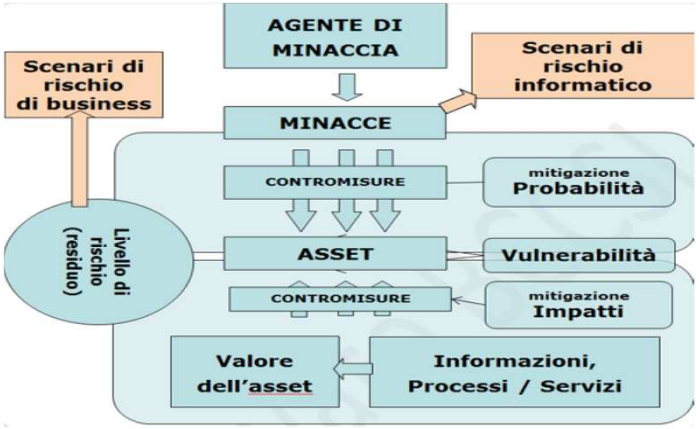
In conformità a quanto previsto dalla Politica di Sicurezza delle Informazioni e alle disposizioni di Banca D'Italia (Circolare n. 285 di Banca D'Italia - ex 263), è stata effettuata l'analisi dei rischi informatici, «Business Impact Analysis (BIA)» e «Technology Chain».

La **probabilità** di accadimento di un evento di rischio viene definito attraverso la frequenza dell'evento (valore quantitativo), sia per la predizione della stessa (valore qualitativo).

L'impatto di un evento di rischio viene valutato sotto il profilo: economico, normativo, strategico, reputazionale.

Piano di trattamento del rischio che descrive le contromisure e le tempistiche di risoluzione.





CYBER SECURITY

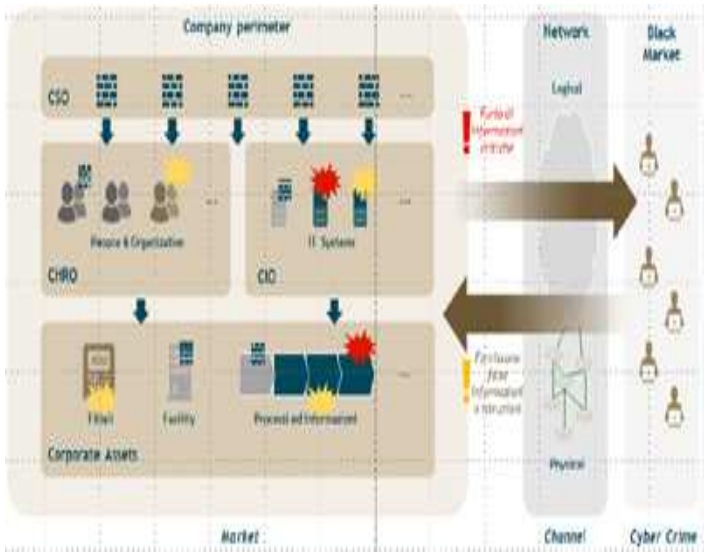
«Security Summit 2016»

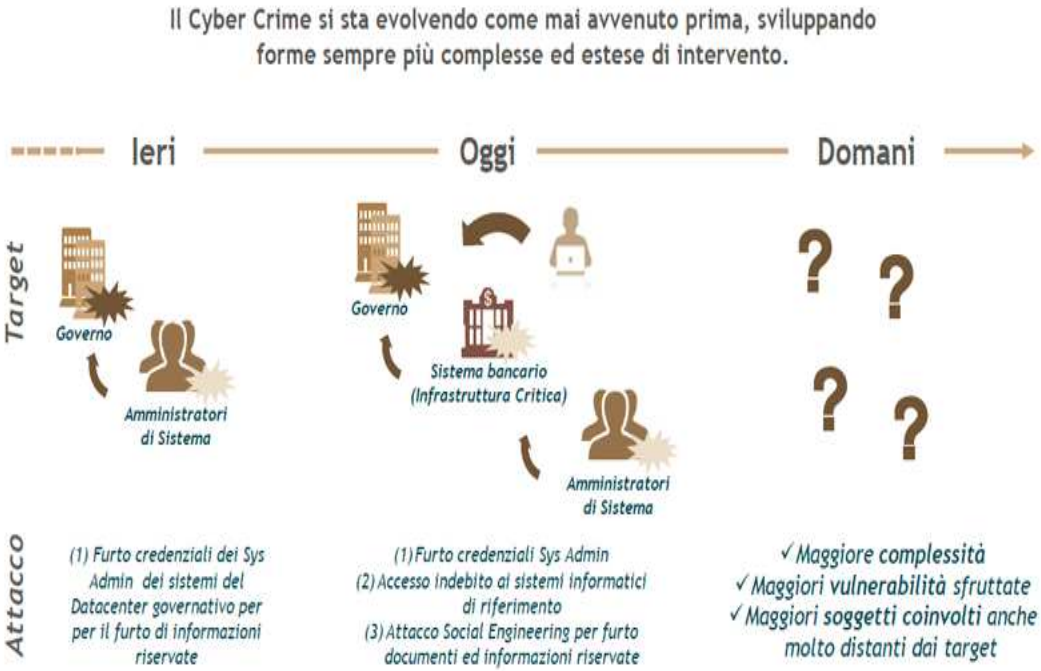
"Lorenzo Possenti"

Milano, 17 marzo 2016

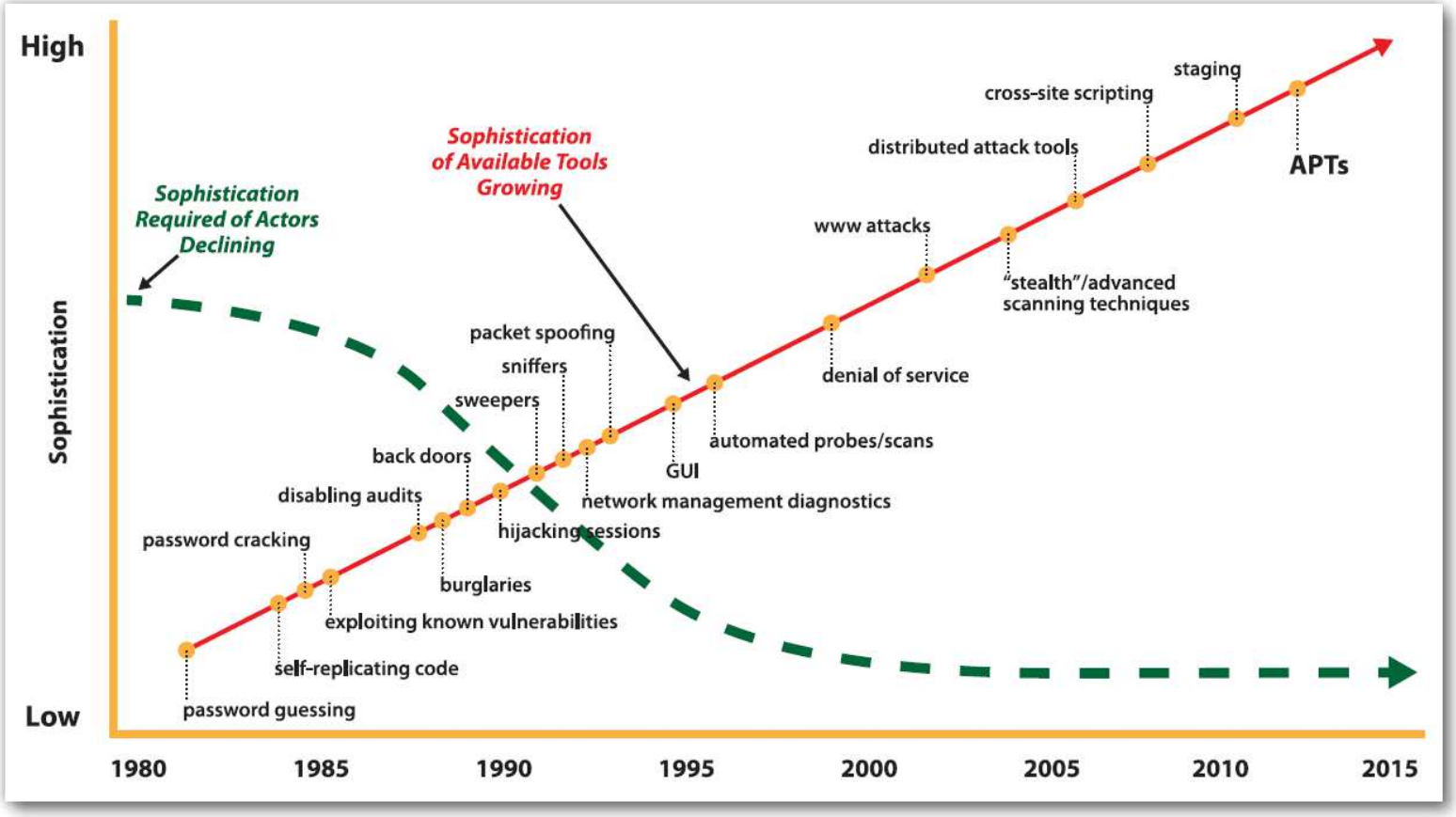
INTERPRETARE LE NUOVE FRONTIERE DEL CYBER CRIME

L'ICT costituisce un contesto in continua evoluzione in cui realtà criminali e non sviluppano metodologie sempre più complesse per portare avanti attività malevole.
È sempre più evidente che la prevenzione ed il contrasto al fenomeno della criminalità digitale sia da giocarsi sui livelli nazionale e internazionali vista la globalità che ormai caratterizza questo genere di minaccia.

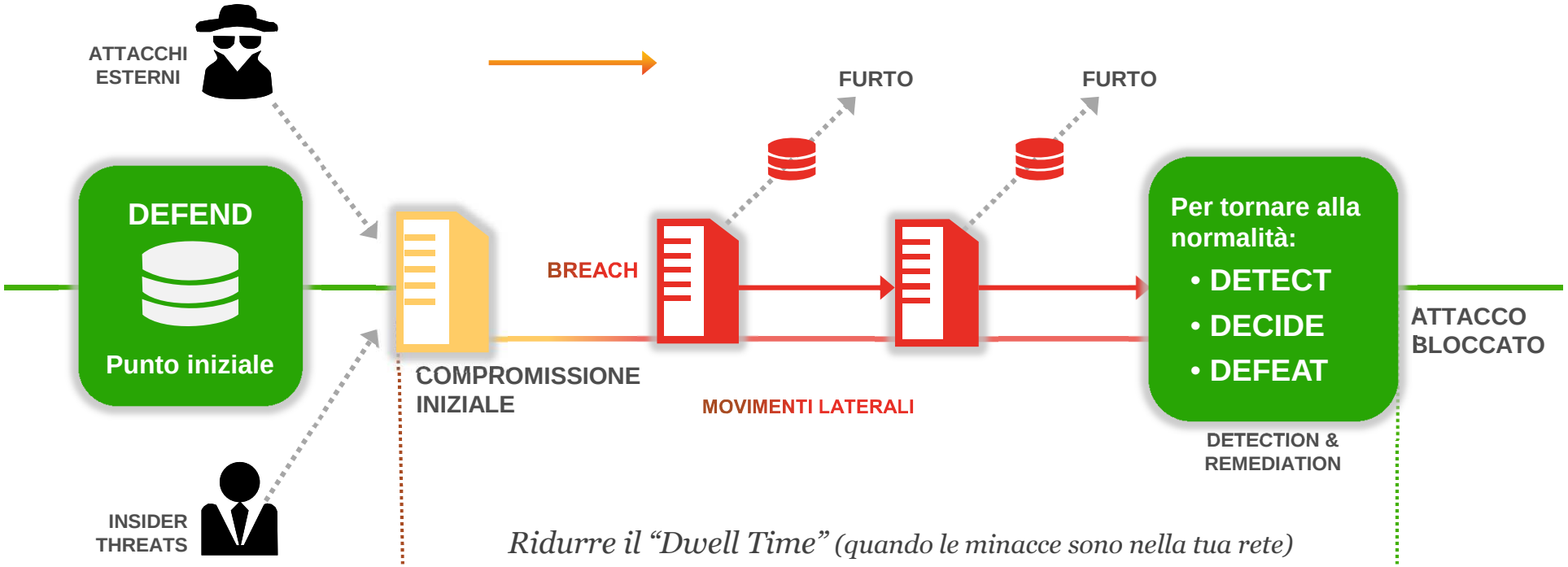




Crescita della complessità del cyberthreat



Quali sono le sfide da affrontare



Ridurre il "Dwell Time" (quando le minacce sono nella tua rete) per minimizzare furti e danni

Le minacce principali

Attacchi visibili

Ransomware

- Evidenti
- Dannosi
- Gli utenti sono la chiave

Attacchi invisibili

APT

- Invisibili
- Devastanti
- Mirano al core business
- Mirati

Utenti

Dati

- Storage Online
- Mail personali
- Collaboration

Crescita della complessità del cyberthreat

- Progetto fallimentare tra il 2007 ed il 2009;
- Ripresi nel 2013 sono diventati una minaccia formidabile;
- Cryptolocker è stato il primo ransomware di nuova generazione;
- Decine di malware locker sono attivi sul mercato;
- Dal 2015 disponibili anche come MAAS (Malware-as-a-Service).

APT e Banche

- Carbanak
- Korkow
- Dyre e Dridex
- Miliardi di euro di danni a Banche e clienti

Nazione	Attacchi	Unici	Utenti ban	Infettati
Switzerland	783	782	0	31
Germany	170	170	0	12
France	158	157	0	9
Unknown	163	163	0	4
Austria	30	29	0	3
United Kingdom	16	15	1	2
Italy	27	27	0	2
Europe	14	13	1	1
Senegal	12	12	0	1
Lithuania	3	3	0	1
Sweden	4	3	0	1
Bosnia and Herzegovina	1	1	0	1
Nigeria	3	3	0	1
China	1	1	0	0

http://www.corriere.it/tecnologia/economia-digitale/15_febbraio_18/carnabak-cyberfurto-secolo-banche-italiane-8250af8a-b787-11e4-bef5-103489912308.shtml

L'evoluzione dell'utente e cosa ci minaccia

- L'utente è cambiato meno di quanto crediamo e continua a capire poco di quello che sta usando;
- Associa a quello che fa lo stesso livello di sicurezza del luogo in cui si trova;
- La tecnomediazione riduce il livello di importanza delle azioni.

CONCLUSIONI

«Security Summit 2016»

“Lorenzo Possenti”

Milano, 17 marzo 2016

Il monitoraggio e alcune protezioni

- BCCSI protegge le proprie Banche attraverso un monitoraggio delle comunicazioni verticali dei malware verso Internet;
- BCCSI ha attivato i sistemi IPS e IDS (Intrusion Prevention & Detection System) installati sui propri firewall e monitora ogni comunicazione da e verso Internet, per identificare attacchi e comunicazioni provenienti anche da macchine compromesse;
- Un sistema di DTP (Data Threat Protection), integrato identifica flussi dati anomali su base comportamentale;
- Da ultimo il DLP (Data Loss Prevention) rileva l'utilizzo scorretto di informazioni riservate a maggior tutela dei nostri clienti;
- Attivazione del SOC (Security Operations Center).

FINE

PRESENTAZIONE