

L'evoluzione della Sicurezza Fisica: un approccio globale

Dalla Physical Security alla Cyber Physical Security: un nuovo percorso strategico

Pietro Blengino
Security Relationship Manager

Milano, 26 maggio 2016

QUALI SONO LE NUOVE SFIDE?

Tutto ci appare a portata di mano, profondamente interconnesso



PERCHE' NON POSSIAMO NON COGLIERLE?

Elemento di continuità importante è la necessità di un accesso fisico al bancomat

TYUPKIN

PADPIN

SKIMER

PLOUTUS

The image shows a composite of digital content related to ATM security. At the top left is a screenshot of a Wired article titled "Bancomat e cybercriminali, 150 milioni di danni in 6 mesi" by Giuditta Mosca, published on April 27, 2016. The article discusses the rise of digital attacks on ATMs and the need for updated software and systems. Below this is a screenshot of the Infosec Institute website featuring a video titled "Hacking ATMs: The New Wave of Malware" posted on October 21, 2014. To the right is a screenshot of a TechEconomy page with a video titled "BONUS- BLACK HAT- Barnaby Jack - Jackpotting Automated..." and a section titled "ATM MALWARE". This section explains that Tyupkin is a malware designed to take control of ATMs and create a backdoor accessible via a PIN pad, allowing criminals to withdraw cash. A sidebar on the right of the TechEconomy page lists various social media posts related to cybersecurity.

Internet ha rivoluzionato le nostre vite e i comportamenti

Il legislatore, per garantire una maggiore sicurezza ed efficienza, introduce una nuova prospettiva della normativa di riferimento

Si passa da un quadro composto da:

- art. 2087 codice civile
- d. lgs. 81/2008
- standard tecnici/normative UNI/EN
- artt. 624, 628 e 640 codice penale

... a un quadro normativo molto più completo, articolato e complesso

- **Direttiva Europea su Cybersecurity**
 - **Decreto del Presidente del Consiglio dei Ministri 24 gennaio 2013**
 - **Decreto Ministero dell'Interno 9 gennaio 2008**
 - **art. 615 ter c.p. accesso abusivo a sistema informatico**
 - **Circolare Banca d'Italia 263 del 27 dicembre 2006**
 - **Sent. Corte Cassazione 29/4/2016**
-

Direttiva Europea su Cybersecurity

- necessità di armonizzare la normativa che altrimenti impedisce economie di scala
 - migliorare la cooperazione tra gli Stati Membri in materia di cybersecurity
 - richiedere agli operatori dei servizi essenziali nei settori dell'energia, dei trasporti, delle banche e della salute nonché dei servizi digitali quali motori di ricerca e cloud computing, per adottare appropriate misure di sicurezza e report sugli eventi/incidenti alle Autorità Nazionali
-
- *Decreto del Presidente del Consiglio dei Ministri 24 gennaio 2013*
 - *Decreto Ministero dell'Interno 9 gennaio 2008*
 - *art. 615 ter c.p. accesso abusivo a sistema informatico*
 - *Circolari Banca d'Italia n. 263 del 27 dicembre 2006 "Nuove disposizioni di vigilanza prudenziale per le banche" e n. 285 del 17 dicembre 2013 "Disposizioni di vigilanza per le banche"*
 - *Sent. Corte Cassazione 29/4/2016*

- *Direttiva Europea su Cybersecurity*
- *Decreto del Presidente del Consiglio dei Ministri 24 gennaio 2013*
- **Decreto Ministero dell'Interno 9 gennaio 2008**
 - Individuazione delle Infrastrutture critiche
 - Accordi di collaborazione con Telecom, ACI, Poste Italiane, ENAV, TERNA, Vodafone, Ferrovie dello Stato, UniCredit, Intesa San Paolo, ABI, Banca d'Italia, SIA SSB, ENI, LEONARDO, ENEL, CONSOB, ANSA, ATM-Milano, ATAC
 - Istituzione del C.N.A.I.P.I.C.
- *art. 615 ter c.p. accesso abusivo a sistema informatico*
- *Circolari Banca d'Italia n. 263 del 27 dicembre 2006 "Nuove disposizioni di vigilanza prudenziale per le banche" e n. 285 del 17 dicembre 2013 "Disposizioni di vigilanza per le banche"*
- *Sent. Corte Cassazione 29/4/2016*

-
- Direttiva Europea su Cybersecurity
 - Decreto del Presidente del Consiglio dei Ministri 24 gennaio 2013
 - Decreto Ministero dell'Interno 9 gennaio 2008
 - art. 615 ter c.p. accesso abusivo a sistema informatico
 - Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.
 - la giurisprudenza fa riferimento a condanne da parte di soggetti autorizzati all'accesso al sistema ma ne hanno fatto un uso illegittimo
 - *Circolari Banca d'Italia 263 del 27 dicembre 2006 e 285 del 17 dicembre 2013*
 - Sent. Corte Cassazione 29/4/2016
-

-
- Direttiva Europea su Cybersecurity
 - Decreto del Presidente del Consiglio dei Ministri 24 gennaio 2013
 - Decreto Ministero dell'Interno 9 gennaio 2008
 - art. 615 ter c.p. accesso abusivo a sistema informatico
 - **Circolari Banca d'Italia n. 263 del 27 dicembre 2006 "Nuove disposizioni di vigilanza prudenziale per le banche" e n. 285 del 17 dicembre 2013 "Disposizioni di vigilanza per le banche"**
 - misure di sicurezza dei sistemi informatici
 - come viene valutata l'affidabilità del Sistema
 - Sent. Corte Cassazione 29/4/2016
-

-
- *Direttiva Europea su Cybersecurity*
 - *Decreto del Presidente del Consiglio dei Ministri 24 gennaio 2013*
 - *Decreto Ministero dell'Interno 9 gennaio 2008*
 - *art. 615 ter c.p. accesso abusivo a sistema informatico*

 - *Circolari Banca d'Italia n. 263 del 27 dicembre 2006 "Nuove disposizioni di vigilanza prudenziale per le banche" e n. 285 del 17 dicembre 2013 "Disposizioni di vigilanza per le banche"*

 - **Sent. Corte Cassazione 29/4/2016**
 - autorizzazione all'uso all'utilizzo di “captatori informatici” – il virus Trojan – all'interno di dispositivi elettronici portatili (ad es., personal computer, tablet, smartphone ecc.).
-

DALLA NUOVA NORMATIVA EMERGONO ALCUNE PAROLE CHIAVE

- Resilienza
- Collaborazione pubblico-privato per lo scambio di informazioni
- Tutela della libertà e dei diritti individuali

QUALI SONO I NOSTRI TARGET DA PROTEGGERE?

L'approccio globale si propone di dare una risposta complessiva e congruente ai principali target di riferimento



LA SICUREZZA DEVE GUARDARE ALLA CONVERGENZA DI SOLUZIONI



IL CONCETTO CHIAVE E' INTEROPERABILITA'

Fondamentale diventa la capacità di una tecnologia o di un sistema di interagire e funzionare con soluzioni o sistemi complessi, esistenti o ancora in divenire, senza alcuna restrizione



LE INFORMAZIONI DISPONIBILI, SE LAVORATE CORRETTAMENTE...



Segnali e allarmi filiale 1



Segnali e allarmi filiale N



Total # Events recorded in the last 60 minutes in Italy: 602

Branches

date	code	description	events
2019-10-13T12:57:30.000+02:00	13712	Roma Rio	allarme generale, allarme generale 1, allarme allarme 1
2019-10-13T12:56:10.000+02:00	13712	Roma Testaccio	allarme 1
2019-10-13T12:56:02.000+02:00	13712	Colle della Rotonda	in via Veneto, in via Veneto
2019-10-13T12:54:13.000+02:00	13712	Roma Torre Angiole	allarme allarme 1, allarme allarme 1, allarme allarme 1
2019-10-13T12:48:38.000+02:00	13712	Roma Capuana	allarme 1
2019-10-13T12:38:37.000+02:00	13712	Roma Tor de Schiavi	allarme 1
2019-10-13T12:36:48.000+02:00	13712	Roma Castro S	allarme 1
2019-10-13T12:15:13.000+02:00	13712	Roma Andrea Doria	allarme generale, allarme generale, allarme generale, allarme generale 1, allarme allarme 1

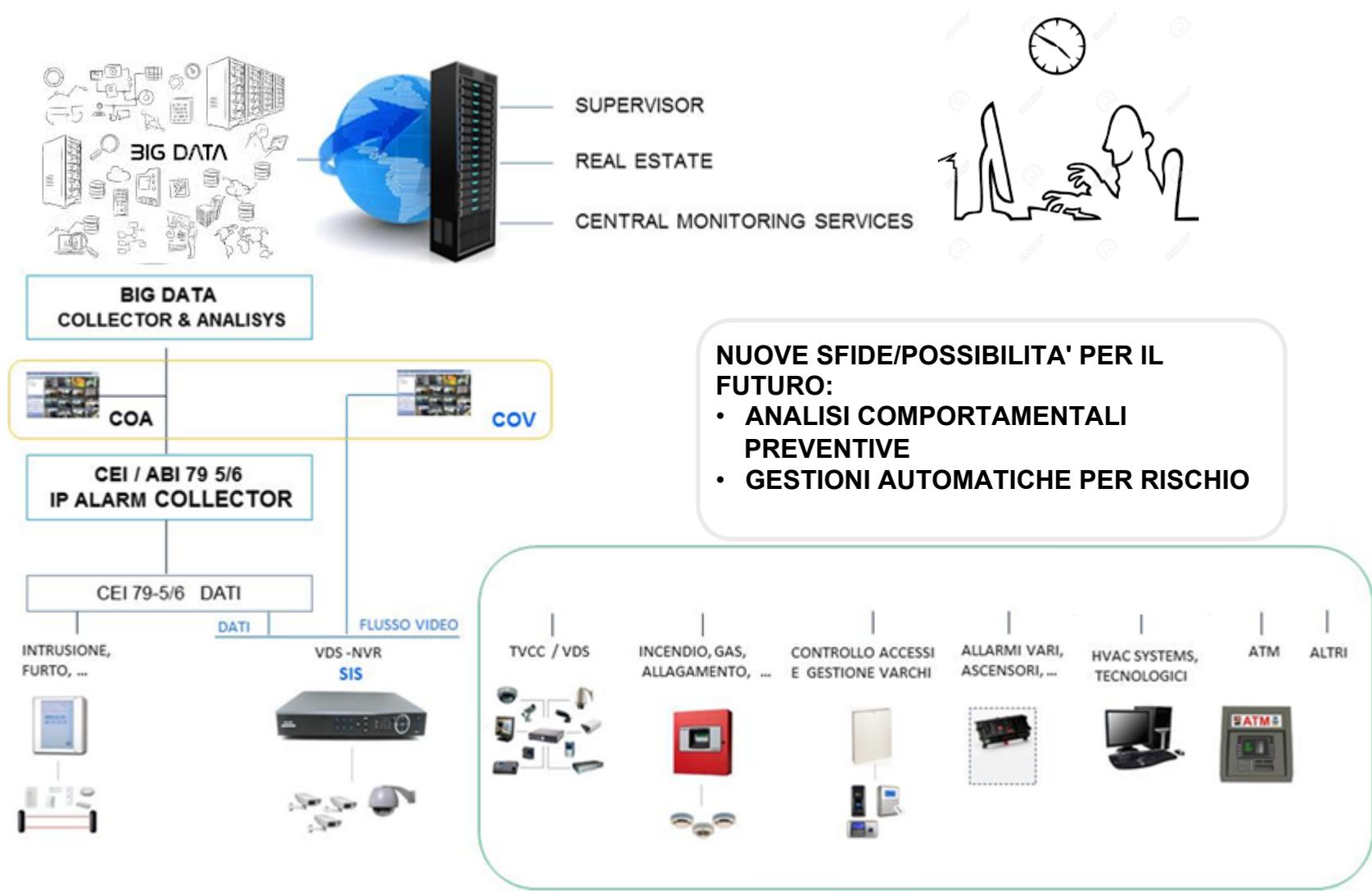


Direzione



Centrale Allarmi

... CONSENTONO UN LIVELLO DI CONTROLLO SENZA PRECEDENTI



*NIENTE E' PIU' IRRESISTIBILE DI
UN'IDEA IL CUI TEMPO SIA
GIUNTO*

V. HUGO