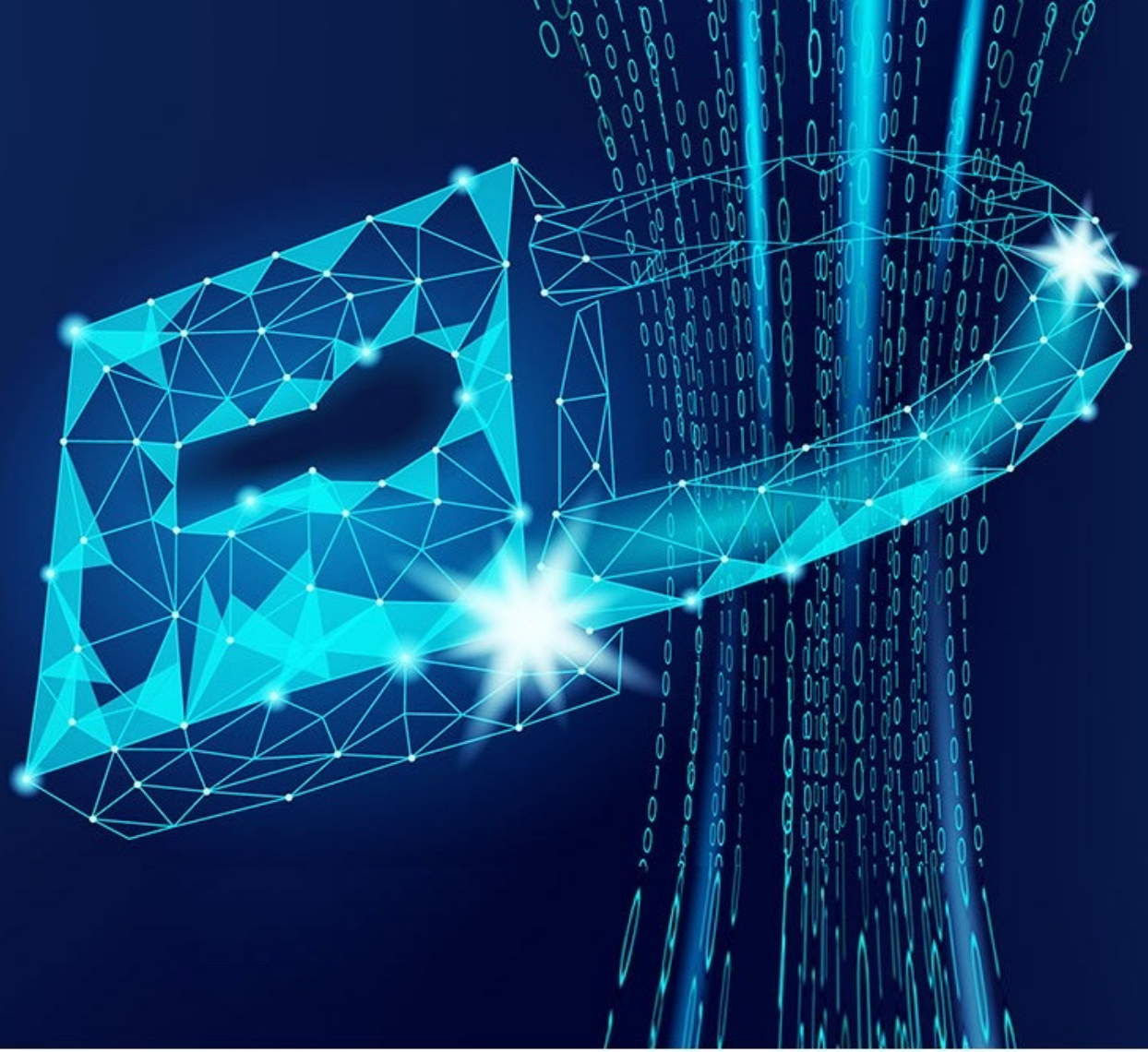


Luca **Leonessi**

Presidente di CyberLabs

19 Maggio 2021

CITEL
Open-PSIM leadership

CyberLabs

Con il Patrocinio di:

A.I.PRO.S.
ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA

A.N.I.V.P.
ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

Evento riconosciuto

ICMQ

CERSA

I 6 PILASTRI DELLA DIGITAL TRANSFORMATION

1	Customer experience interna ed esterna
2	Persone: il cuore della trasformazione
3	Cambiamento e resilienza
4	Innovazione culturale, manageriale, tecnologica...
5	Leadership, volontà di evolversi e migliorare
6	Cultura del cambiamento

Physical Security

Cyber Security

Security è Innovazione

MAI PIÙ SOLI®

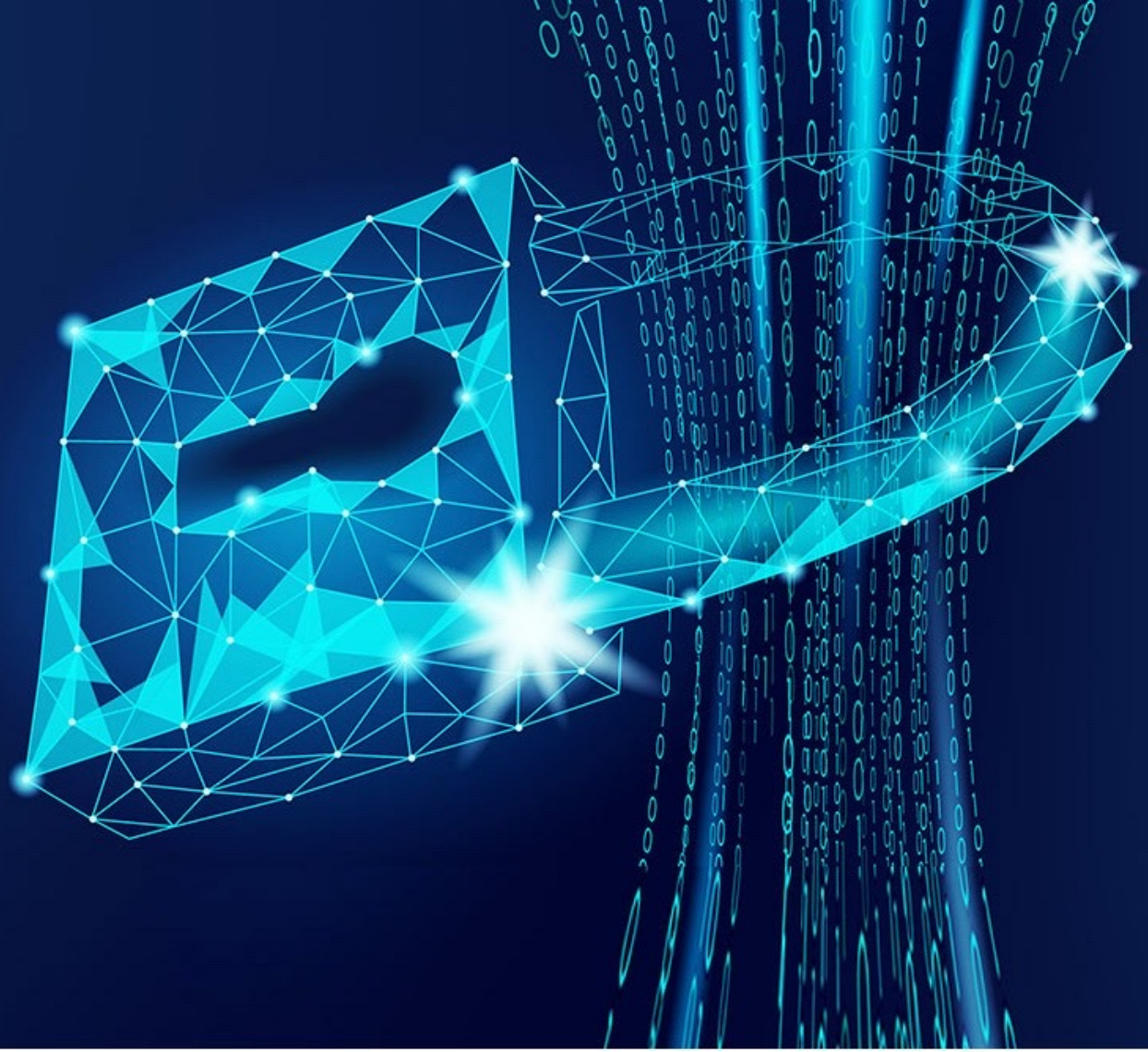
SECUR SHOP
VIDEOALLARME | ANTIRAPINA

Data Analysis

GecomData

LABORATORIO PER LA SICUREZZA

GRAZIE!



CITEL
Open-PSIM leadership

CyberLabs

Con il Patrocinio di:

A.I.PRO.S.
ASSOCIAZIONE ITALIANA
PROFESSIONISTI DELLA SICUREZZA

A.N.I.V.P.
ASSOCIAZIONE NAZIONALE
ISTITUTI DI VIGILANZA PRIVATA
E SERVIZI FIDUCIARI DI SICUREZZA

Evento riconosciuto

ICMQ

CERSA

Sicurezza cibernetica e protezione dei dati: ratio e obiettivi degli interventi normativi

Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

CITEL
Open-PSIM leadership

CyberLabs

con il Patrocinio di:

A.I.PRO.S.
ASSOCIAZIONE ITALIANA
PROFESSIONISTI DELLA SICUREZZA

A.N.I.V.P.
ASSOCIAZIONE NAZIONALE
ISTITUTI DI VIGILANZA PRIVATA
E SERVIZI FIDUCIARI DI SICUREZZA

Sicurezza cibernetica e protezione dei dati: ratio e obiettivi degli interventi normativi

Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

- *La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un **diritto fondamentale*** (considerando 1- GDPR)
- *Il trattamento dei dati personali dovrebbe essere al **servizio** dell'uomo* (considerando 4 - GDPR)
- *La rapidità dell'**evoluzione tecnologica** e la **globalizzazione** comportano nuove sfide per la protezione dei dati personali* (considerando 6 - GDPR)

Crime is finding new ways. With the help of malicious software, it is possible to take control over a large number of computers and steal credit card numbers, find sensitive information or launch large-scale attacks. It is time for us to step up our efforts against cyber crime, also often used by organised crime. The proposals we are putting forward today are one important step, as we criminalise the creation and selling of malicious software and improve European police cooperation.

(Cecilia Malmström, commissaria europea per gli Affari Interni, 2010)

Sicurezza cibernetica e protezione dei dati: ratio e obiettivi degli interventi normativi

Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

Data Protection: quadro normativo.

- Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995

Legge n. 675 del 31 dicembre 1996

D.Lgs. n. 196 del 30 giugno 2003 (Codice Privacy)

- **Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (in vigore dal 24 Maggio 2016 – applicabile dal 25 Maggio 2018) - GDPR**

D.Lgs. n. 101 del 10 agosto 2018 che ha modificato il D.Lgs. 196/2003

- Proposta di Regolamento relativo alla governance europea dei dati (Atto sulla governance dei dati) – Commissione UE 25/11/2020

Sicurezza cibernetica e protezione dei dati: ratio e obiettivi degli interventi normativi

Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

Cyber Security: quadro normativo.

- **Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale e al Comitato delle regioni «Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo» (2001)**
- **Proposta di Direttiva in materia di cyber crime (Commissione Europea, 30 settembre 2010)**
- **Proposta di Regolamento per rafforzare e modernizzare la European Network and information Security Agency (ENISA) (Commissione europea, 30 settembre 2010)**
- **Istituzione del Centro Europeo per la lotta alla criminalità informatica (9 gennaio 2013 – European Police Office – Europol)**

enisa
European Network and Information Security Agency

Sicurezza cibernetica e protezione dei dati: ratio e obiettivi degli interventi normativi

Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

- **Piano di sicurezza informatica dell'UE per tutelare l'internet aperta, la libertà e le opportunità nella rete (Commissione Europea, 7 febbraio 2013)**
  - **strategia sulla sicurezza informatica**
  - **proposta di direttiva in materia di sicurezza delle reti e dell'informazione**
  - **definizione di cyber security**

- **direttiva (UE) 2016/1148 sulla sicurezza delle reti e dei sistemi informativi nell'Unione (Direttiva NIS) del 6 luglio 2016 ► recepita in Italia con D.Lgs. n. 65 del 18 maggio 2018**

- **Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019, relativo all'ENISA e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione**

Sicurezza cibernetica e protezione dei dati: ratio e obiettivi degli interventi normativi

Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

D.L. n. 105 del 21 settembre 2019

"Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica"

- **Legge di conversione n. 133 del 18 novembre 2019**
- **D.L. 163/2019 (modifiche), legge di conversione 8/2020 – D.L. 76/2020 (modifiche), legge di conversione 120/2020**
- **DPCM 30/07/2020 n. 131, pubblicato in Gazzetta Ufficiale il 20/10/2020, *Regolamento-quadro in materia di perimetro di sicurezza nazionale cibernetica in esecuzione del D.L. 105/2019***
- **29/01/2021 il Consiglio dei Ministri approva il decreto attuativo che rende operativo il Centro di Valutazione e Certificazione Nazionale (CVCN) – istituito presso il Ministero dello Sviluppo Economico – e gli altri centri di valutazione (CV) chiamati ad effettuare verifiche e valutazioni dei beni, dei sistemi e dei servizi ICT**

- **In corso: esame dello schema di DPCM relativo ad un Regolamento per la notifica degli incidenti che hanno impatto su reti, sistemi informativi e servizi informatici**
- **Atteso: DPCM che definisca i criteri tecnici per l'individuazione delle categorie dei beni, dei sistemi e dei servici ICT che saranno oggetto di valutazione da parte del CVCN e dei CV**
- **Atteso: DPCM che definisca i criteri di accreditamento dei laboratori di cui il CVCN potrà avvalersi per espletare le proprie funzioni**

Reati informatici: dalla definizione all'applicazione. Casi di giurisprudenza e criticità quotidiane.

Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

CITEL
Open-PSIM leadership

CyberLabs

con il Patrocinio di:

A.I.PRO.S.
ASSOCIAZIONE ITALIANA
PROFESSIONISTI DELLA SICUREZZA

A.N.I.V.P.
ASSOCIAZIONE NAZIONALE
ISTITUTI DI VIGILANZA PRIVATA
E SERVIZI FIDUCIARI DI SICUREZZA

Reati informatici: dalla definizione all'applicazione. Casi di giurisprudenza e criticità quotidiane.

Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

Reati informatici:
dalla definizione all'applicazione.
Casi di giurisprudenza e criticità quotidiane.

L'evoluzione tecnologica degli ultimi anni ha reso indispensabile l'uso di Internet quale mezzo di scambio di informazioni, di accesso alle grandi banche dati, di esecuzione di transazioni e disposizioni finanziarie, di ideazione e creazione di nuove attività professionali.

La rapida diffusione dell'uso di Internet ha ben presto messo in evidenza i punti di debolezza della Rete stessa, in particolar modo con riferimento alla sicurezza informatica.

(www.commissariatodips.it)

Reati informatici: dalla definizione all'applicazione. Casi di giurisprudenza e criticità quotidiane.

Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

Consiglio d'Europa:

- Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Strasburgo, 28 agosto 1981, in vigore dal 1° ottobre 1985)
- Raccomandazione *«sur la criminalité en relation avec l'ordinateur»,* 13 settembre 1989 *n. R (89) 9*
- Convenzione per la prevenzione del terrorismo (Varsavia, 16 maggio 2005, in vigore dal 1° giugno 2007)
- Convenzione per la protezione dei minori contro lo sfruttamento e gli abusi sessuali (Lanzarote, 25 ottobre 2007, in vigore dal 1° luglio 2010)

Reati informatici: dalla definizione all'applicazione. Casi di giurisprudenza e criticità quotidiane.

Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

- Legge 547/1993 "*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*"

- Legge 48/2008 "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*"

⇣

- art. 24bis D.Lgs. 231/2001 (delitti informatici e trattamento illecito di dati)

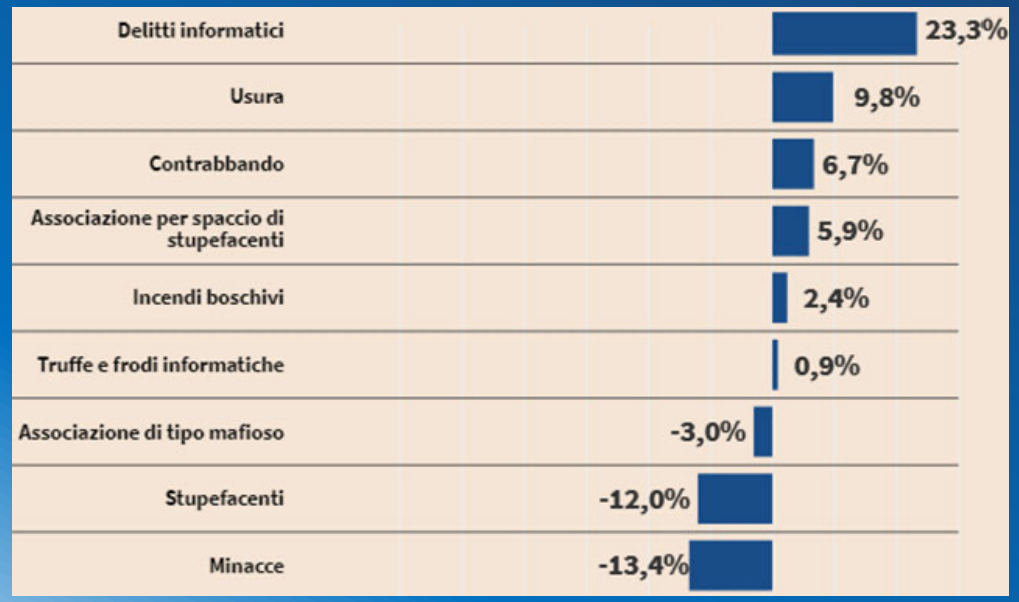
Reati informatici: dalla definizione all'applicazione. Casi di giurisprudenza e criticità quotidiane.

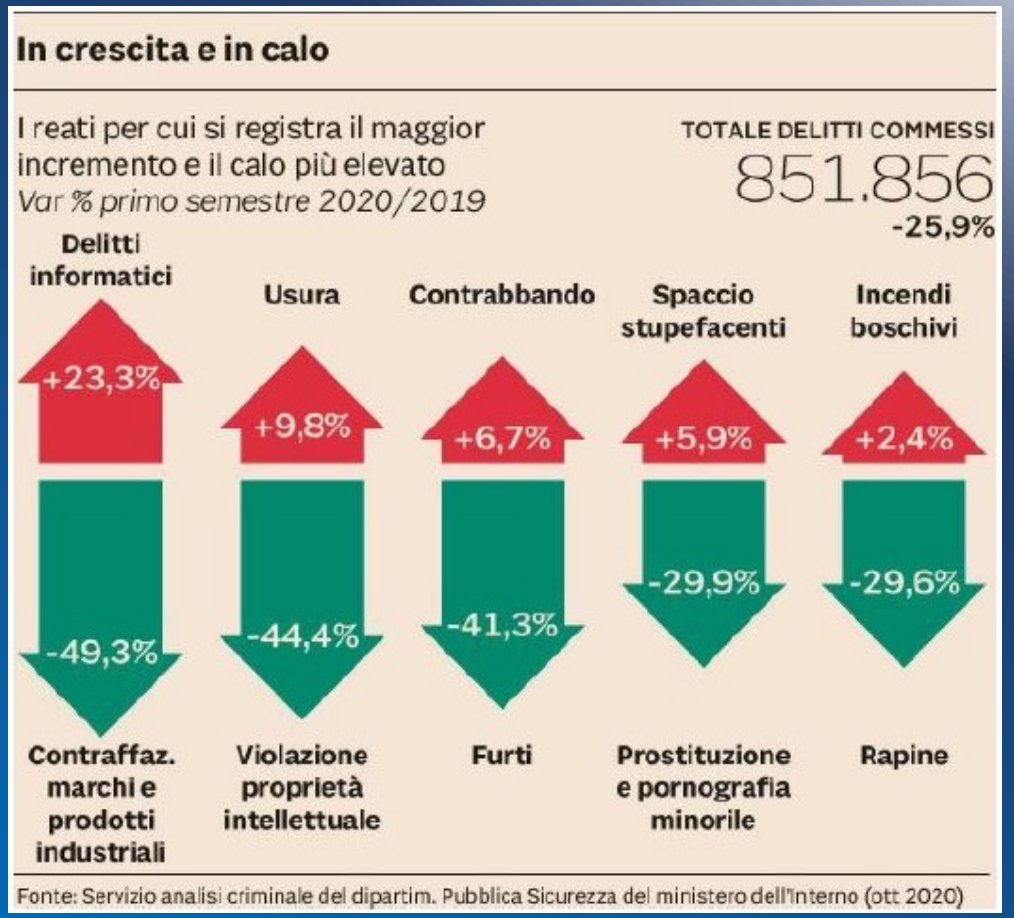
Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

Catherine De Bolle

Reati informatici: dalla definizione all'applicazione. Casi di giurisprudenza e criticità quotidiane.

Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.





Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

Reati contro la fede pubblica.

- **Frode informatica del soggetto che presta servizi di certificazione di firma elettronica** Art. 640-quinquies c.p. ⇒ reato presupposto ex art. 24-bis D.lgs. 231/2001

- **Documenti informatic**i Art.491-bis c.p. ⇒ reato presupposto ex art. 24-bis D.lgs. 231/2001

L'inserimento di dati relativi al superamento di esami mai sostenuti su un supporto informatico, che abbia funzione vicaria dell'archivio dell'Università e, pertanto, destinazione potenzialmente probatoria, quanto meno provvisoria, integra il reato di cui agli artt. 483 e 491 bis (Cass. Pen. 15535/2018)

- **Sostituzione di persona** Art. 494 c.p.

Integra il reato di cui all'art. 494 c.p. la condotta di chi si sostituisca a taluno creando un profilo social indicando l'utenza telefonica di tale persona (Cass. Pen. 652/2020)

Reati informatici: dalla definizione all'applicazione. Casi di giurisprudenza e criticità quotidiane.

Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

Reati contro la sicurezza informatica.

- Frode informatica Art. 640-ter c.p.
- Frode informatica a danno dello Stato o di altro ente pubblico Art. 640-ter i.c.d. Art. 640 co. 2 n. 1 c.p.: ⇒ reato presupposto ex art. 24 D.lgs. 231/2001

Utilizzazione di sistemi di blocco od alterazione della comunicazione telematica tra apparecchi da gioco del tipo slot-machine e l'amministrazione finanziaria, trattandosi di alterazione dell'altrui sistema telematico, finalizzato all'indebito trattenimento della quota di imposta sulle giocate (Cass. Pen. 41767/2017, Cass. Pen. 24634/2018)

Il soggetto che, collegandosi tramite indirizzo IP sul sistema informatico o telematico di Poste Italiane, introduce i dati del c/c intestato a un terzo e dispone un'operazione di ricarica sulla propria postepay (Trib. Napoli 4163/2019)

Condotta di colui che, essendogli stata revocata la delega ad operare sul conto corrente on line, attraverso l'utilizzazione dei codici di accesso telematici penetri abusivamente nel sistema informatico bancario ed effettui la ricarica del telefono cellulare (Cass. Pen. 50140/2015)

Virus che hanno la finalità di carpire dati di accesso a servizi on-line al fine di ottenere profitti ("financial malware", "trojan banking" e ransomware …): le modalità di infezione sono diverse, la più diffusa è il classico allegato al messaggio di posta elettronica celati da false fatture, contravvenzioni, avvisi di consegna pacchi, che giungono in formato .doc .pdf

Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico Art. 615-quinquies c.p. ⇒ reato presupposto ex art. 24-bis D.lgs. 231/2001

malware, spyware, trojan, dialer

i cd. virus benigni che, pur senza avere effetti distruttivi, disturbano il normale funzionamento del sistema, segnalando in vario modo la loro presenza

- Danneggiamento di informazioni, dati e programmi informatici Art. 635-bis c.p. ⇒ reato presupposto ex art. 24-bis D.lgs. 231/2001

integra il delitto in esame la cancellazione di dati informatici, ancorché questi possano essere recuperati attraverso una complessa procedura tecnica che richiede l'uso di particolari sistemi applicativi e presuppone specifiche conoscenze; caso in cui un dipendente aveva cancellato, dal computer affidatogli dal datore di lavoro per motivi lavorativi, un numero rilevante di dati, i cui files erano stati recuperati grazie all'intervento di un tecnico informatico specializzato (Cass. Pen. 8555/2012)

Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica necessità Art. 635-ter c.p. ⇒ reato presupposto ex art. 24-bis D.lgs. 231/2001
- Danneggiamento di sistemi informatici o telematici Art. 635-quater c.p. ⇒ reato presupposto ex art. 24-bis D.lgs. 231/2001
- Danneggiamento di sistemi informatici o telematici di pubblica utilità Art. 635-quinquies c.p. ⇒ reato presupposto ex art. 24-bis D.lgs. 231/2001
- Attentato a impianti di pubblica utilità Art. 420 c.p.
- Esercizio arbitrario delle proprie ragioni con violenza sulle cose Art. 392 comma 3 c.p.

Reati informatici: dalla definizione all'applicazione. Casi di giurisprudenza e criticità quotidiane.

Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

Reati contro la riservatezza informatica.

- Accesso abusivo a un sistema informatico o telematico Art. 615-ter c.p. ⇒ reato presupposto ex art. 24-bis D.lgs. 231/2001

Il reato sussiste anche se l'accesso al sistema è stato determinato da una password facilmente aggirabile e, addirittura, se le credenziali di accesso sono state comunicate all'autore del reato o da questi legittimamente acquisite (*Cass. Pen. 47049/2019 – caso stalking; Cass. Pen. 2905/2018 accesso a profilo facebook altrui*); così, ad esempio, commette il reato il marito che acceda al conto corrente online intestato alla coniuge e compia operazioni qualora la moglie abbia revocato al consorte la delega per le suddette operazioni (*Cass. Pen. 14627/2018; Cass. Pen. 14627/2017*);

Accesso al profilo Facebook altrui: la Corte di Cassazione ha stabilito che, per provare il reato di accesso abusivo al sistema informatico e la sostituzione di persona per chi accede al profilo Facebook di un terzo, può bastare l'identificazione dell'indirizzo Ip, cioè quell'indirizzo numerico che identifica univocamente un dispositivo collegato alla rete;

Commette il reato l'ex-dipendente che, dopo aver rassegnato le dimissioni, s'introduce nel sistema informatico della società, al fine di copiare in un hard disk tutte le cartelle del server dell'azienda (Cass. Pen. 8631/2016)

Integra il reato la condotta del datore di lavoro o del superiore gerarchico che acceda abusivamente alla casella di posta elettronica del dipendente, protetta da una password personalizzata, trattandosi di uno spazio di memoria di un sistema informatico nell'esclusiva disponibilità del suo titolare, identificato da un account registrato presso il provider del servizio (Cass. Pen. 13057/2016)

Condotta del pubblico dipendente, impiegato dell'Agenzia delle entrate, che effettui interrogazioni sul sistema centrale dell'anagrafe tributaria sulla posizione di contribuenti non rientranti, in ragione del loro domicilio fiscale, nella competenza del proprio ufficio (Cass. Pen. 22024/2013);

Reati informatici: dalla definizione all'applicazione. Casi di giurisprudenza e criticità quotidiane.

Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici Art. 615-quater c.p. ⇒ reato presupposto ex art. 24-bis D.lgs. 231/2001

L'illecita acquisizione di codici di accesso a conti correnti bancari e postali ed il loro successivo utilizzo per effettuare prelievi e bonifici online non autorizzati (c.d. phishing) è inquadrabile ai sensi degli artt. 640-ter, 615-quater e 615-quinquies c.p. (Tribunale Milano 28/07/2006)

Integra il reato di detenzione e diffusione abusiva di codici di accesso a servizi informatici o telematici di cui all'art. 615-quater c.p., la condotta di colui che si procuri abusivamente il numero seriale di un apparecchio telefonico cellulare appartenente ad altro soggetto, poiché attraverso la corrispondente modifica del codice di un ulteriore apparecchio (cosiddetta "clonazione") è possibile realizzare una illecita connessione alla rete di telefonia mobile, che costituisce un sistema telematico protetto, anche con riferimento alle banche concernenti i dati esteriori delle comunicazioni, gestite mediante tecnologie informatiche (Cass. Pen. 5688/2004)

Reati informatici: dalla definizione all'applicazione. Casi di giurisprudenza e criticità quotidiane.

Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

- Violazione, sottrazione e soppressione di corrispondenza Art. 616 c.p.

- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche Art. 617-quater c.p. ⇒ reato presupposto ex art. 24-bis D.lgs. 231/2001

Commette il reato di cui all'art. 617-quater c.p. il responsabile del centro elaborazione dati di una società che, pur investito della connessa posizione di amministratore di sistema, avvalendosi di mezzi atti ad eludere i meccanismi di sicurezza volti ad impedire l'accesso di estranei alle comunicazioni (password, firewall, criptazione od altri analoghi strumenti), intercetti le comunicazioni di posta elettronica indirizzate ai singoli amministratori e dipendenti (Cass. Pen. 31135/2007)

- Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche Art. 617-quinquies c.p. ⇒ reato presupposto ex art. 24-bis D.lgs. 231/2001

- Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche Art. 617-sexies c.p.

La responsabilità ex art. 617 sexies c.p. è stata ravvisata nell'invio di false email apparentemente provenienti da un istituto bancario (phishing) (Tribunale Milano, 10/12/2007).

- Rivelazione del contenuto di documenti segreti Art. 621 c.p.

Reati informatici: dalla definizione all'applicazione. Casi di giurisprudenza e criticità quotidiane.

Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

Legge 633/1941, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio.

- **Art. 171, comma 1–a (bis)**
- **Art. 171, comma 3**
- **Art. 171-bis**
- **Art. 171-ter**
- **Art. 171-septies**
- **Art. 171-octies**

- *La copia di pagine HTML da un sito web non protetto da misure di sicurezza riprodotte in un altro sito, può eventualmente costituire violazione della L. 22.4.1941, n. 633 (e succ. mod.) sul diritto d'autore (Trib. Milano 12.12.2006; Cass. Pen. 22319/2003)*

- *Duplicazione abusiva di programmi informatici protetti da copyright:*

✓ *hard disk loading (installazione di copie illegali di software sugli hard disk per facilitare l'acquisto del dispositivo informatico da parte del cliente);*

✓ *contraffazione di software (pirateria che consiste nella duplicazione e vendita illegale di materiale protetto da copyright, riproducendo e imitando tutti gli elementi del prodotto originale);*

- *Abusivo impiego strumentale di prodotti intellettuali, in particolare software:*

✓ *utilizzo di un programma in violazione delle condizioni di licenza;*

✓ *installazione di software monoutente su più elaboratori aziendali;*

✓ *adesione a offerte di aggiornamento del programma, pur in assenza di una copia legale dello stesso.*

Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

GDPR e D.Lgs. 196/2003

ART. 83 GDPR: sanzioni amministrative

- **comma 4 > sanzione amministrativa pecuniaria fino a € 10.000.000 o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per violazioni delle disposizioni in materia di:**

art. 25, privacy by design and privacy by default

art. 28, responsabile del trattamento

art. 29, incaricato del trattamento

art. 30, registro dei trattamenti

art. 32, misure di sicurezza

art. 33, notifica di violazione

art. 34, comunicazione di violazione all'interessato

art. 37 e ss., designazione DPO e suoi compiti

- …

- **comma 5 > sanzione amministrativa pecuniaria fino a € 20.000.000 o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per violazioni delle disposizioni in materia di:**

artt. 12-13-14, informative all'interessato

art. 15, diritto di accesso dell'interessato

art. 16, diritto di rettifica

art. 17, diritto alla cancellazione / all'oblio

Paola Finetto – Avvocato. Data Protection Officer, componente di Organismi di Vigilanza ex D.Lgs. 231/2001.

- **ART. 84 GDPR: altre sanzioni previste dalla normativa nazionale**

- **D.Lgs. 196/2003 ss.mm., artt. 167, 167bis, 167ter, ~~168, 170, 171, 172~~**

Art. 167 *(Trattamento illecito di dati)*

Art. 167-bis *(Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala)*

Art. 167-ter *(Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala)*

Phalanx MK2: Le vulnerabilità delle reti e dei sistemi in un contesto 4.0: come monitorare e migliorare la superficie di attacco.

Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group

CITEL
Open-PSIM leadership

CyberLabs

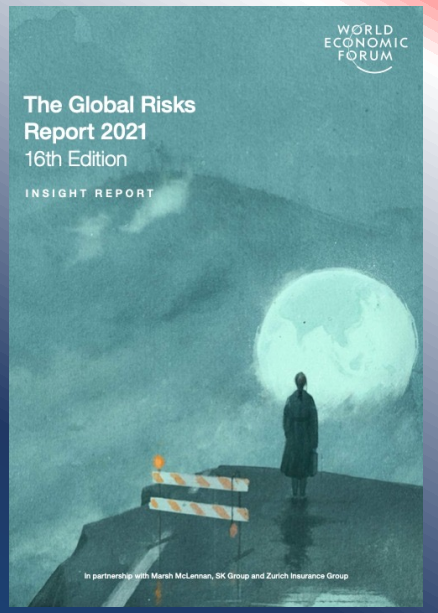
con il Patrocinio di:

A.I.PRO.S.
ASSOCIAZIONE ITALIANA
PROFESSIONISTI DELLA SICUREZZA

A.N.I.V.P.
ASSOCIAZIONE NAZIONALE
ISTITUTI DI VIGILANZA PRIVATA
E SERVIZI FIDUCIARI DI SICUREZZA

Phalanx MK2: Le vulnerabilità delle reti e dei sistemi in un contesto 4.0: come monitorare e migliorare la superficie di attacco.

Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group



Top Risks by likelihood

1. Extreme weather
2. Climate action failure
3. Human environmental damage
4. Infectious diseases
5. Biodiversity loss
6. Digital power concentration
7. Digital inequality
8. Interstate relations fracture
9. Cybersecurity failure
10. Livelihood crises

Top Risks by impact

1. Infectious diseases
2. Climate action failure
3. Weapons of mass destruction
4. Biodiversity loss
5. Natural resource crises
6. Human environmental damage
7. Livelihood crises
8. Extreme weather
9. Debt crises
10. IT infrastructure breakdown

CITEL Open-PSIM leadership
CyberLabs
con il Patrocinio di:
A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA
A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

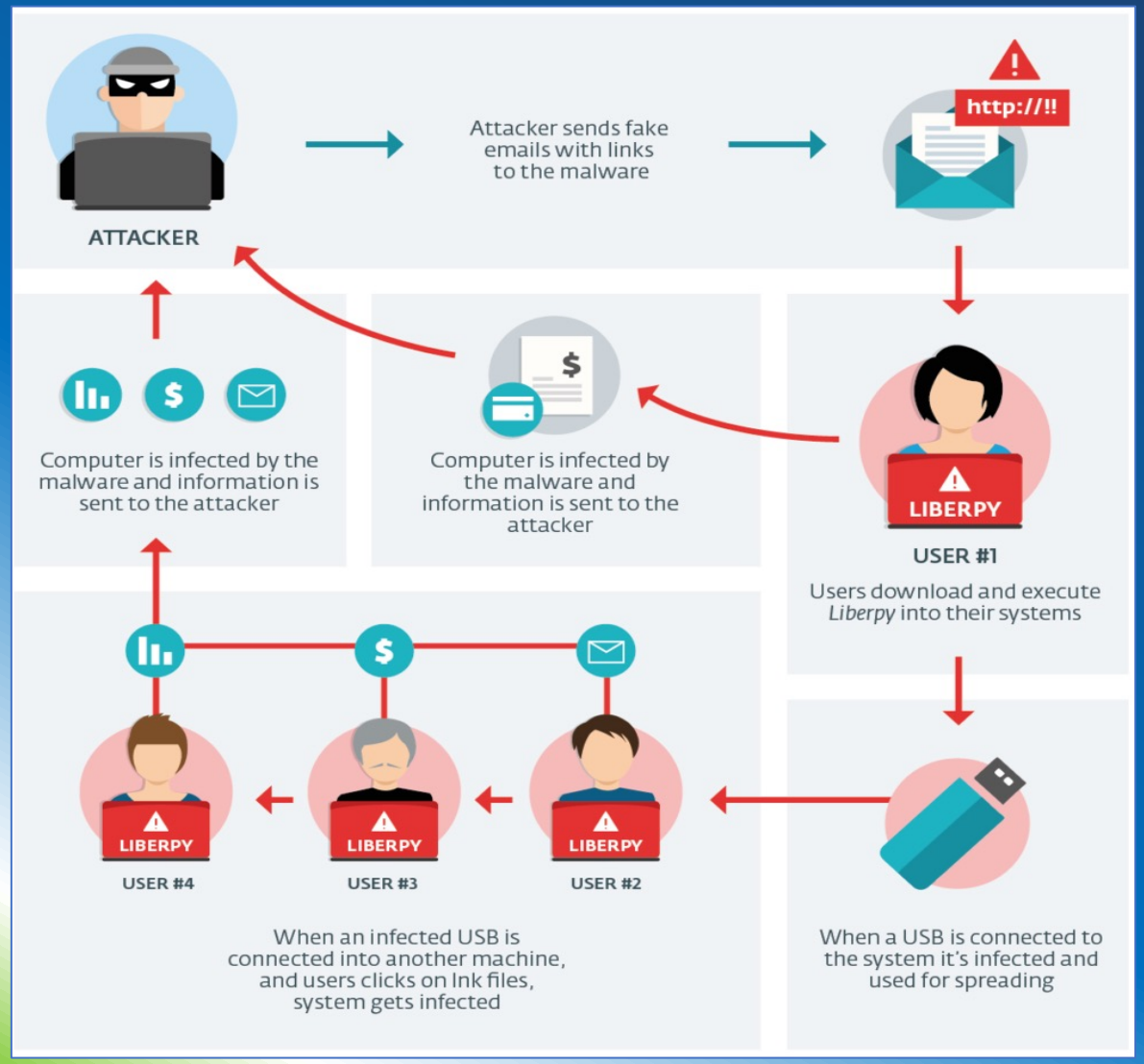
Phalanx MK2: Le vulnerabilità delle reti e dei sistemi in un contesto 4.0: come monitorare e migliorare la superficie di attacco.

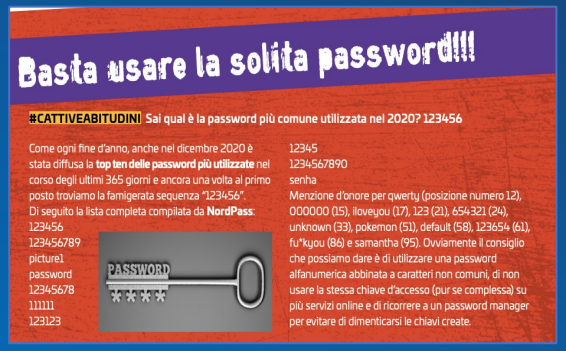
Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group

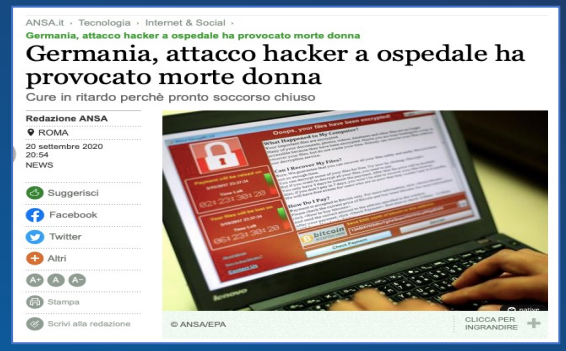
con il Patrocinio di:

Phalanx MK2: Le vulnerabilità delle reti e dei sistemi in un contesto 4.0: come monitorare e migliorare la superficie di attacco.

Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group







CITEL Open-PSIM leadership

CyberLabs

con il Patrocinio di:

A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA

A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

Phalanx MK2: Le vulnerabilità delle reti e dei sistemi in un contesto 4.0: come monitorare e migliorare la superficie di attacco.

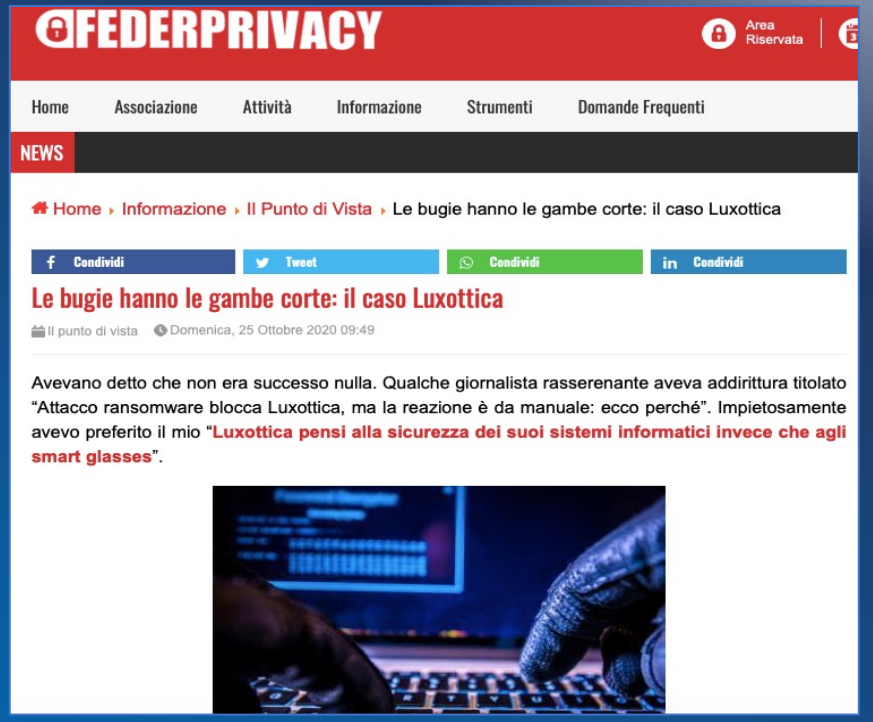
Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group

MENU CERCA IL GAZZETTINO.it

Attacco hacker alla Luxottica: tutti i dipendenti, da Agordo alla Cina, lasciati a casa

NORDEST > BELLUNO

Lunedì 21 Settembre 2020


FEDERPRIVACY Area Riservata

Home Associazione Attività Informazione Strumenti Domande Frequenti

NEWS

Home › Informazione › Il Punto di Vista › Le bugie hanno le gambe corte: il caso Luxottica

Condividi Tweet Condividi Condividi

Le bugie hanno le gambe corte: il caso Luxottica

Il punto di vista Domenica, 25 Ottobre 2020 09:49

Avevano detto che non era successo nulla. Qualche giornalista rasserenante aveva addirittura titolato "Attacco ransomware blocca Luxottica, ma la reazione è da manuale: ecco perché". Impietosamente avevo preferito il mio "**Luxottica pensi alla sicurezza dei suoi sistemi informatici invece che agli smart glasses**".

CITEL Open-PSIM leadership

CyberLabs

con il Patrocinio di:

A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA

A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

Phalanx MK2: Le vulnerabilità delle reti e dei sistemi in un contesto 4.0: come monitorare e migliorare la superficie di attacco.

Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group

Articolo 32
EU RGPD
"Sicurezza del trattamento"

=> Motivo: 83, 74, 75, 76, 77
=> administrative fine: Art. 83 (4) lit a

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
=> Articolo: 24

a) la pseudonimizzazione e la cifratura dei dati personali;
=> Articolo: 4

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
=> Motivo: 75

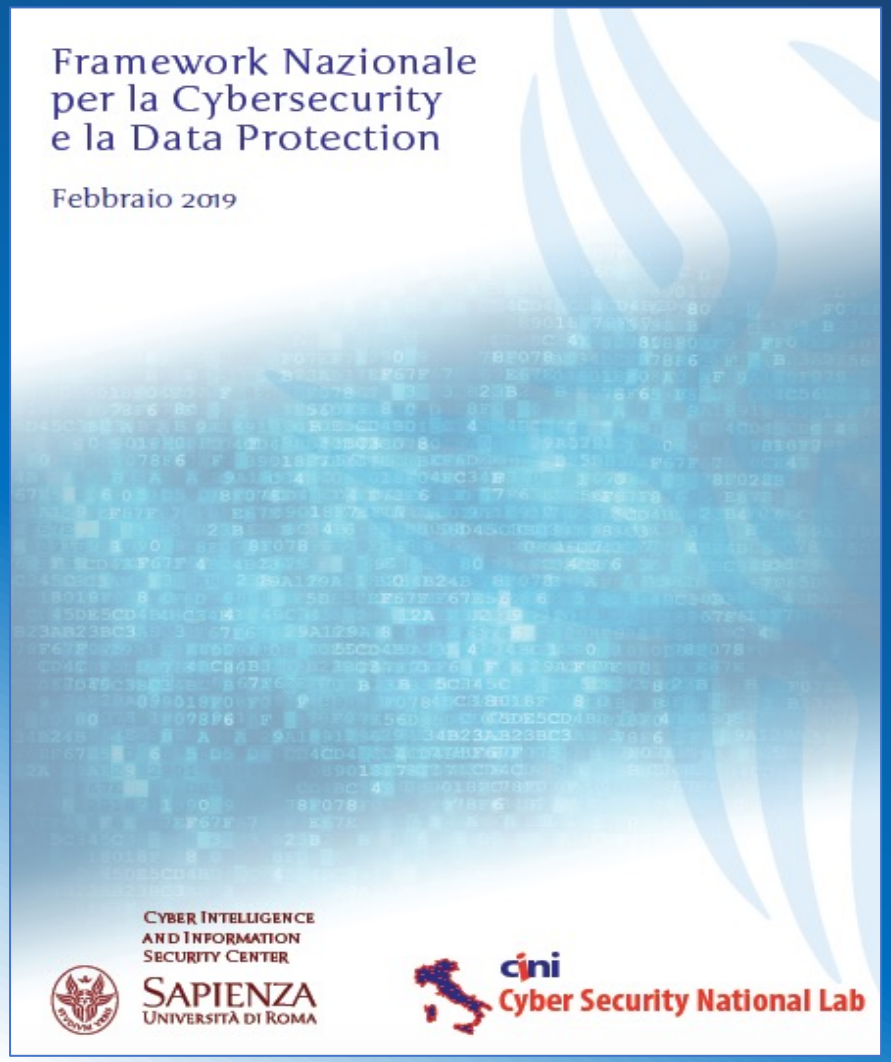
3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.
=> Articolo: 29

CITEL Open-PSIM leadership
CyberLabs
con il Patrocinio di:
A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA
A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

Phalanx MK2: Le vulnerabilità delle reti e dei sistemi in un contesto 4.0: come monitorare e migliorare la superficie di attacco.

Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group



Con il supporto dell'Autorità Garante per la Protezione dei Dati Personali e del Dipartimento delle Informazioni per la Sicurezza della Presidenza del Consiglio dei Ministri.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

CITEL
Open-PSIM leadership

CyberLabs

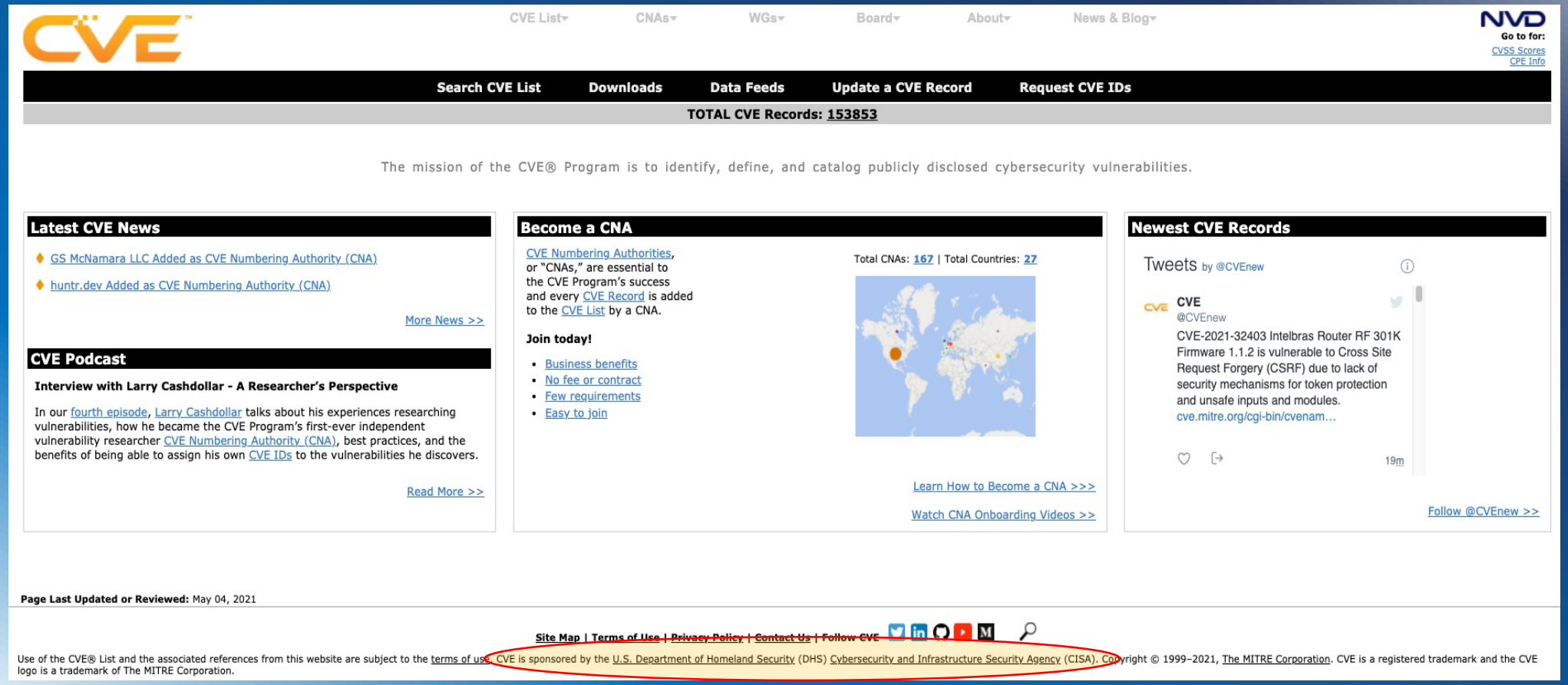
con il Patrocinio di:

A.I.PRO.S.
ASSOCIAZIONE ITALIANA
PROFESSIONISTI DELLA SICUREZZA

A.N.I.V.P.
ASSOCIAZIONE NAZIONALE
ISTITUTI DI VIGILANZA PRIVATA
E SERVIZI FIDUCIARI DI SICUREZZA

Phalanx MK2: Le vulnerabilità delle reti e dei sistemi in un contesto 4.0: come monitorare e migliorare la superficie di attacco.

Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group



CITEL Open-PSIM leadership

CyberLabs

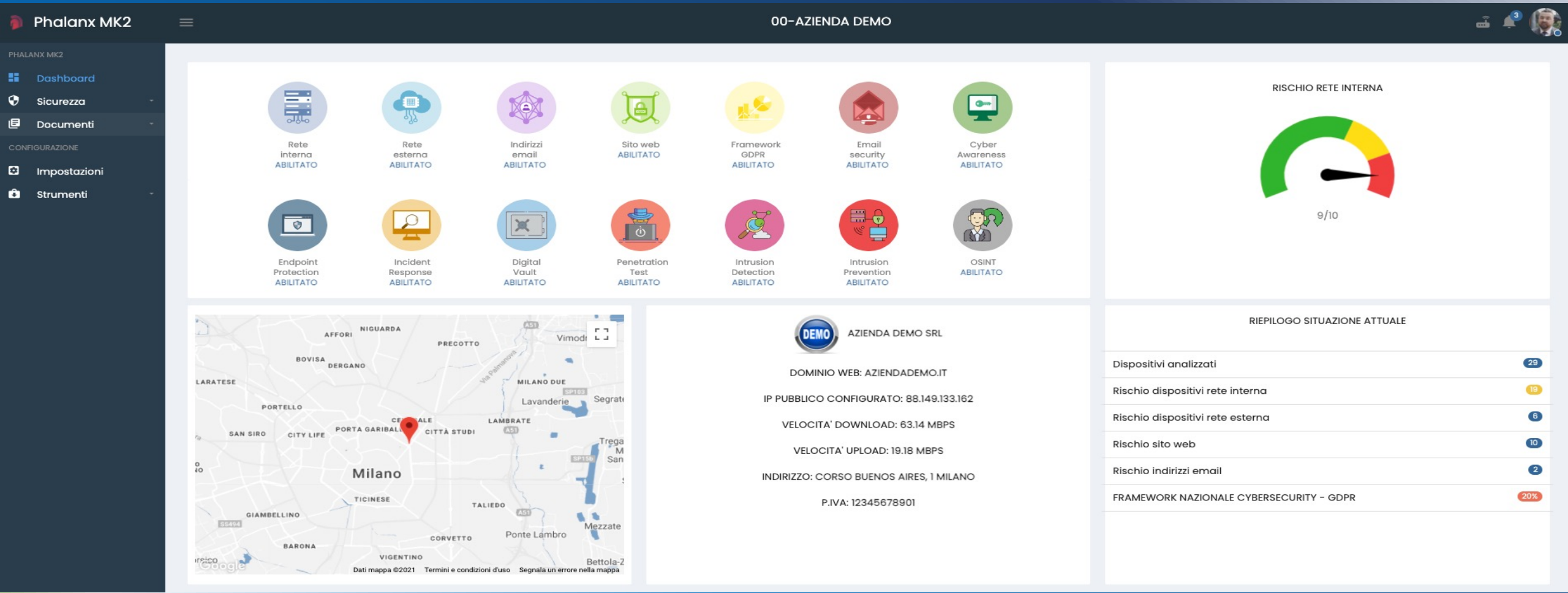
con il Patrocinio di:

A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA

A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

Phalanx MK2: Le vulnerabilità delle reti e dei sistemi in un contesto 4.0: come monitorare e migliorare la superficie di attacco.

Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group



CITEL Open-PSIM leadership

CyberLabs

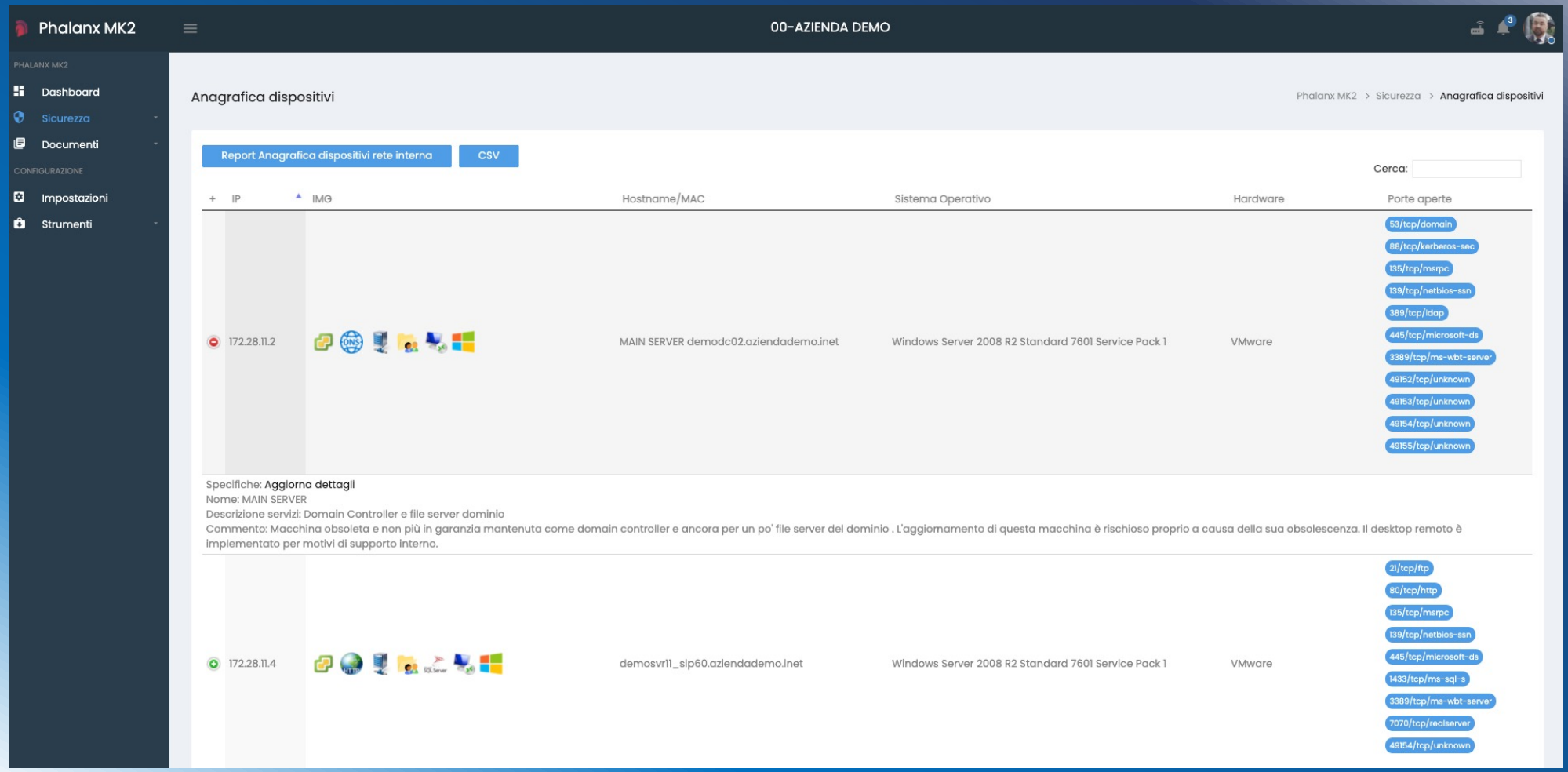
con il Patrocinio di:

A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA

A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

Phalanx MK2: Le vulnerabilità delle reti e dei sistemi in un contesto 4.0: come monitorare e migliorare la superficie di attacco.

Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group



CITEL Open-PSIM leadership

CyberLabs

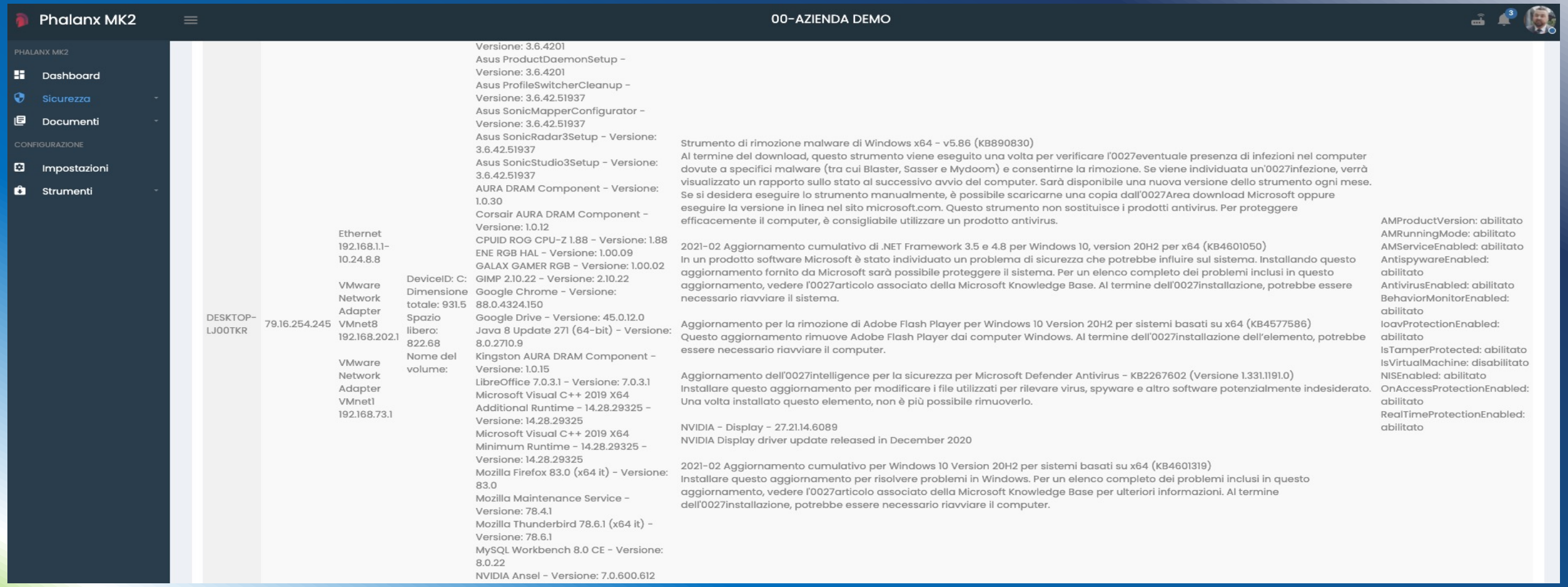
con il Patrocinio di:

A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA

A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

Phalanx MK2: Le vulnerabilità delle reti e dei sistemi in un contesto 4.0: come monitorare e migliorare la superficie di attacco.

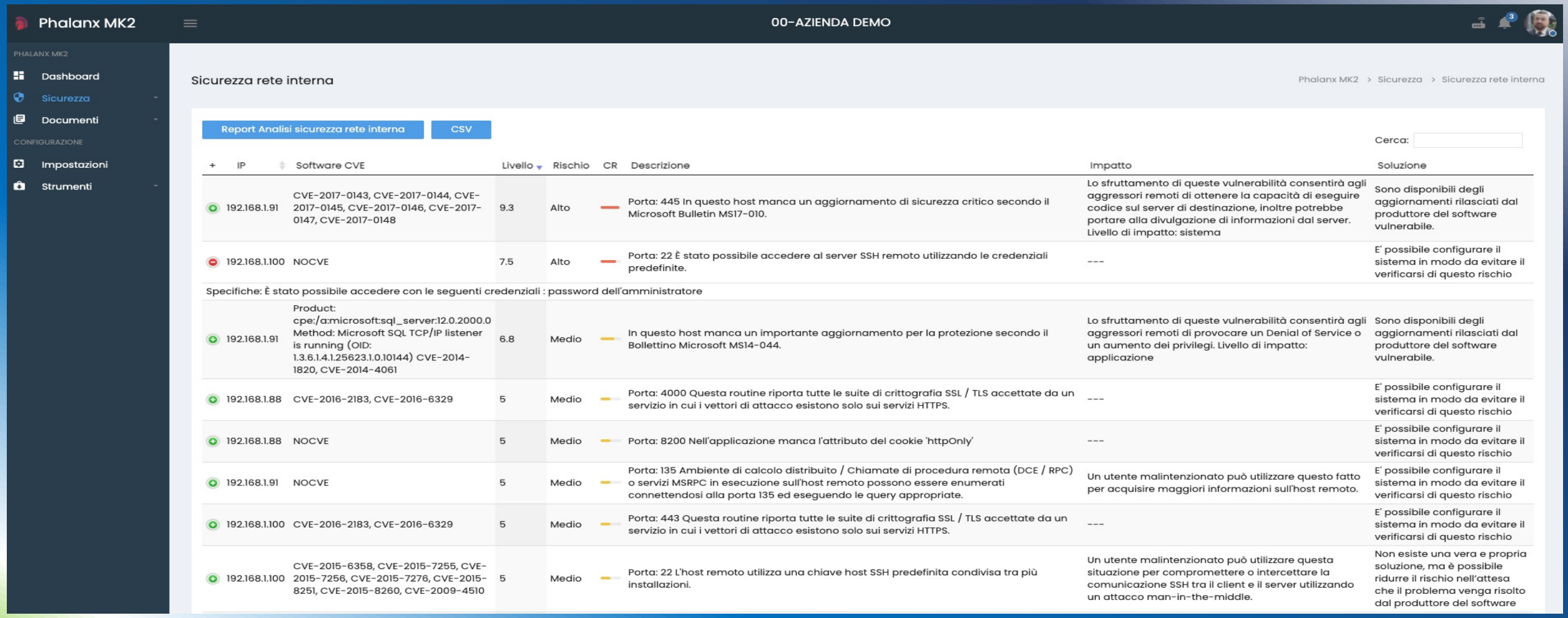
Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group



CITEL Open-PSIM leadership
CyberLabs
con il Patrocinio di:
A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA
A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

Phalanx MK2: Le vulnerabilità delle reti e dei sistemi in un contesto 4.0: come monitorare e migliorare la superficie di attacco.

Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group

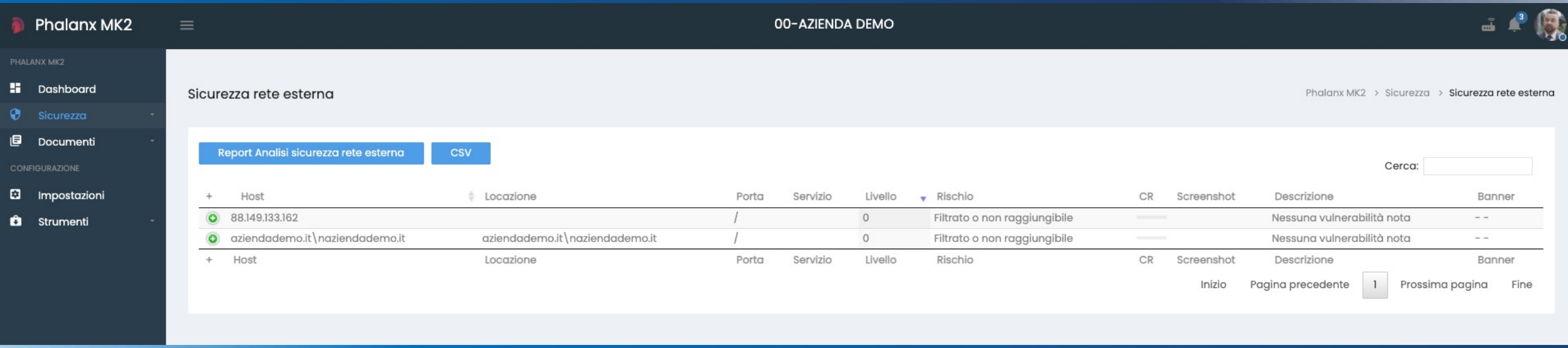


+	IP	Software CVE	Livello	Rischio	CR	Descrizione	Impatto	Soluzione
	192.168.1.91	CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148	9.3	Alto		Porta: 445 In questo host manca un aggiornamento di sicurezza critico secondo il Microsoft Bulletin MS17-010.	Lo sfruttamento di queste vulnerabilità consentirà agli aggressori remoti di ottenere la capacità di eseguire codice sul server di destinazione, inoltre potrebbe portare alla divulgazione di informazioni dal server. Livello di impatto: sistema	Sono disponibili degli aggiornamenti rilasciati dal produttore del software vulnerabile.
	192.168.1.100	NOCVE	7.5	Alto		Porta: 22 È stato possibile accedere al server SSH remoto utilizzando le credenziali predefinite.	---	E' possibile configurare il sistema in modo da evitare il verificarsi di questo rischio
Specifiche: È stato possibile accedere con le seguenti credenziali : password dell'amministratore								
	192.168.1.91	Product: cpe:/a:microsoft:sql_server:12.0.2000.0 Method: Microsoft SQL TCP/IP listener is running (OID: 1.3.6.1.4.1.25623.1.0.10144) CVE-2014-1820, CVE-2014-4061	6.8	Medio		In questo host manca un importante aggiornamento per la protezione secondo il Bollettino Microsoft MS14-044.	Lo sfruttamento di queste vulnerabilità consentirà agli aggressori remoti di provocare un Denial of Service o un aumento dei privilegi. Livello di impatto: applicazione	Sono disponibili degli aggiornamenti rilasciati dal produttore del software vulnerabile.
	192.168.1.88	CVE-2016-2183, CVE-2016-6329	5	Medio		Porta: 4000 Questa routine riporta tutte le suite di crittografia SSL / TLS accettate da un servizio in cui i vettori di attacco esistono solo sui servizi HTTPS.	---	E' possibile configurare il sistema in modo da evitare il verificarsi di questo rischio
	192.168.1.88	NOCVE	5	Medio		Porta: 8200 Nell'applicazione manca l'attributo del cookie 'httpOnly'	---	E' possibile configurare il sistema in modo da evitare il verificarsi di questo rischio
	192.168.1.91	NOCVE	5	Medio		Porta: 135 Ambiente di calcolo distribuito / Chiamate di procedura remota (DCE / RPC) o servizi MSRPC in esecuzione sull'host remoto possono essere enumerati connettendosi alla porta 135 ed eseguendo le query appropriate.	Un utente malintenzionato può utilizzare questo fatto per acquisire maggiori informazioni sull'host remoto.	E' possibile configurare il sistema in modo da evitare il verificarsi di questo rischio
	192.168.1.100	CVE-2016-2183, CVE-2016-6329	5	Medio		Porta: 443 Questa routine riporta tutte le suite di crittografia SSL / TLS accettate da un servizio in cui i vettori di attacco esistono solo sui servizi HTTPS.	---	E' possibile configurare il sistema in modo da evitare il verificarsi di questo rischio
	192.168.1.100	CVE-2015-6358, CVE-2015-7255, CVE-2015-7256, CVE-2015-7276, CVE-2015-8251, CVE-2015-8260, CVE-2009-4510	5	Medio		Porta: 22 L'host remoto utilizza una chiave host SSH predefinita condivisa tra più installazioni.	Un utente malintenzionato può utilizzare questa situazione per compromettere o intercettare la comunicazione SSH tra il client e il server utilizzando un attacco man-in-the-middle.	Non esiste una vera e propria soluzione, ma è possibile ridurre il rischio nell'attesa che il problema venga risolto dal produttore del software

CITEL Open-PSIM leadership
CyberLabs
con il Patrocinio di:
A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA
A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

Phalanx MK2: Le vulnerabilità delle reti e dei sistemi in un contesto 4.0: come monitorare e migliorare la superficie di attacco.

Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group



CITEL Open-PSIM leadership

CyberLabs

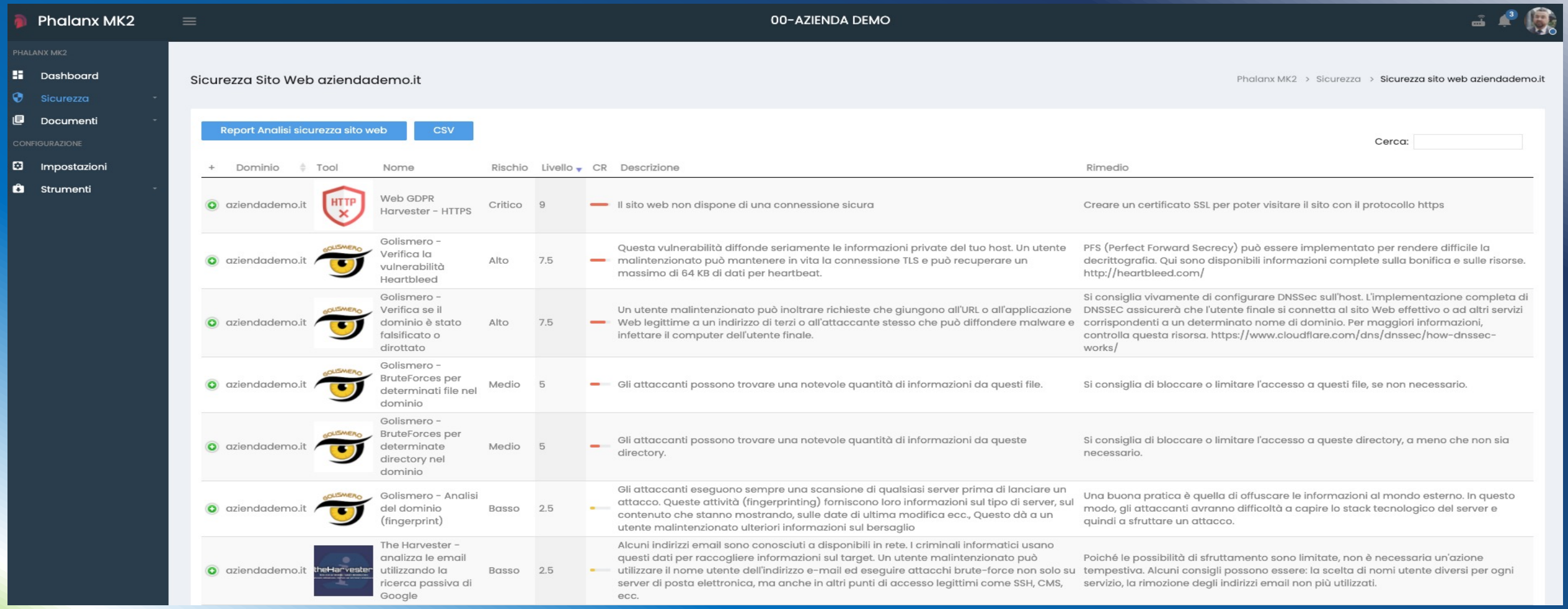
con il Patrocinio di:

A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA

A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

Phalanx MK2: Le vulnerabilità delle reti e dei sistemi in un contesto 4.0: come monitorare e migliorare la superficie di attacco.

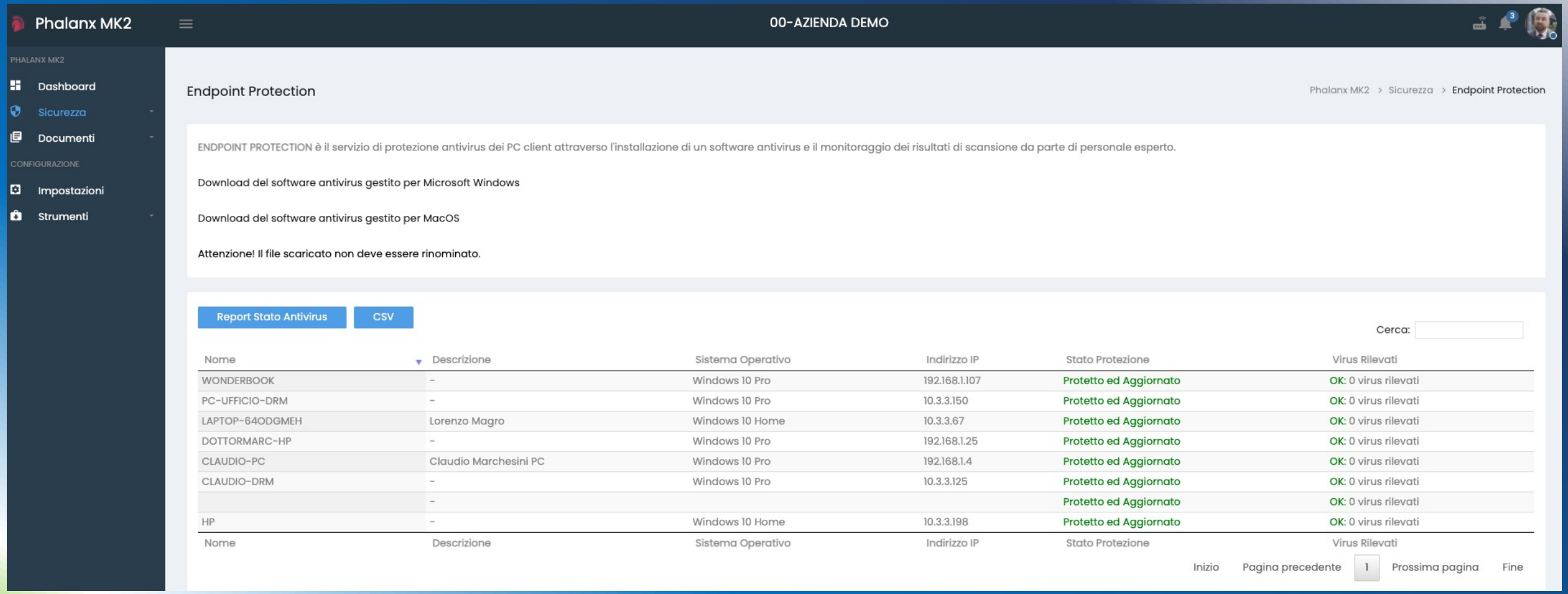
Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group



CITEL Open-PSIM leadership
CyberLabs
con il Patrocinio di:
A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA
A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

Phalanx MK2: Le vulnerabilità delle reti e dei sistemi in un contesto 4.0: come monitorare e migliorare la superficie di attacco.

Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group



CITEL Open-PSIM leadership

CyberLabs

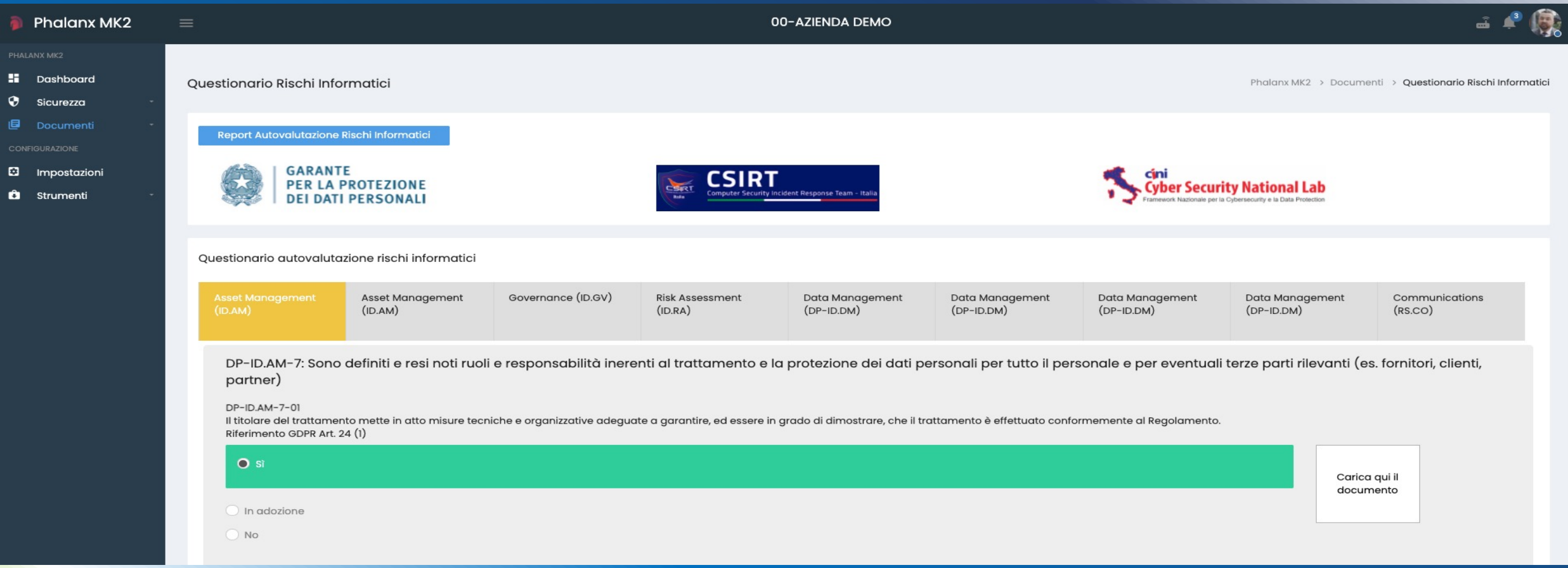
con il Patrocinio di:

A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA

A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

Phalanx MK2: Le vulnerabilità delle reti e dei sistemi in un contesto 4.0: come monitorare e migliorare la superficie di attacco.

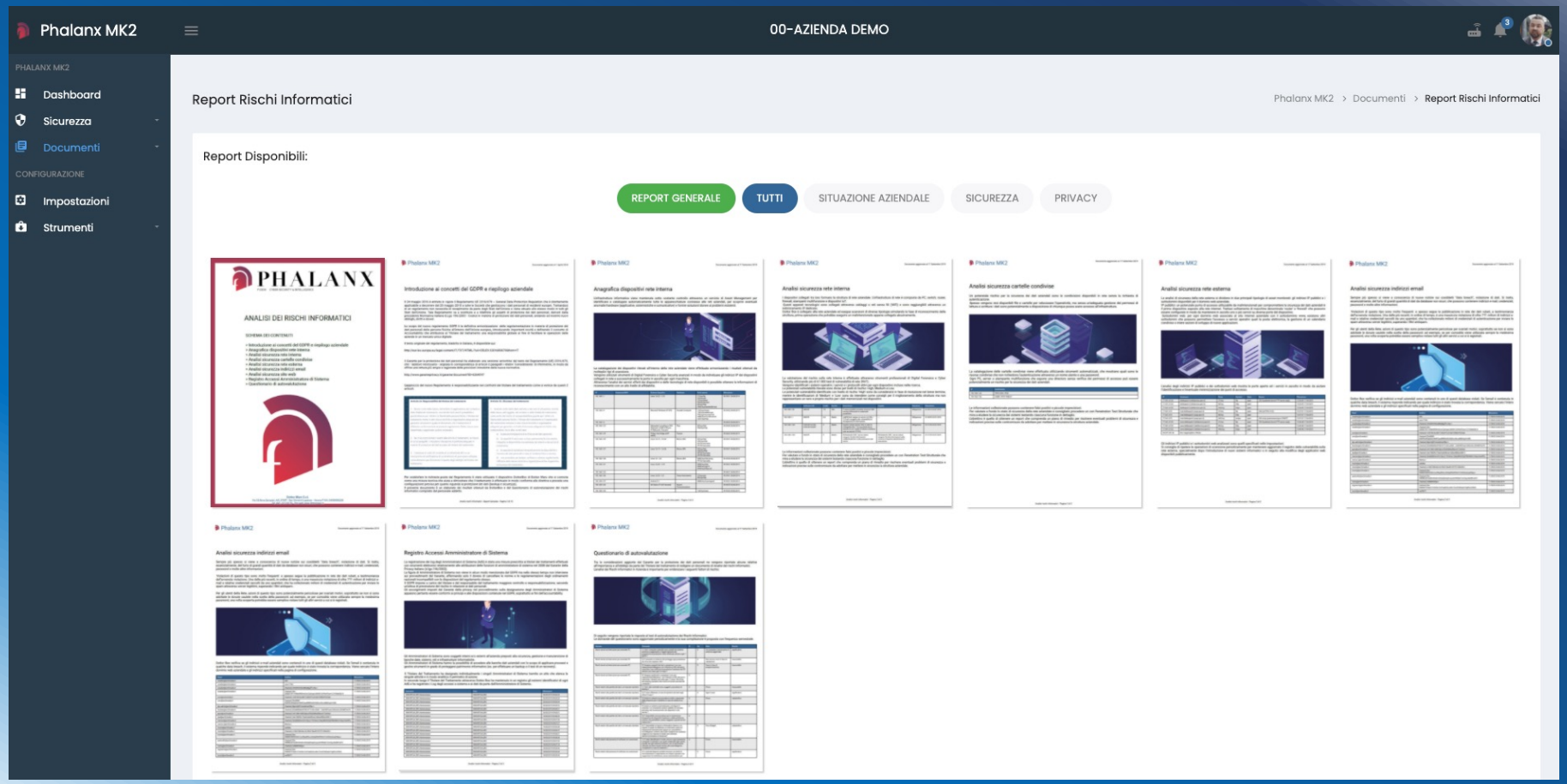
Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group



CITEL Open-PSIM leadership
CyberLabs
con il Patrocinio di:
A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA
A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

Phalanx MK2: Le vulnerabilità delle reti e dei sistemi in un contesto 4.0: come monitorare e migliorare la superficie di attacco.

Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group



con il Patrocinio di:

CITEL Open-PSIM leadership

CyberLabs

A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA

A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

Phalanx MK2: Data Breach & Incident Response Management.

Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group

CITEL
Open-PSIM leadership

CyberLabs

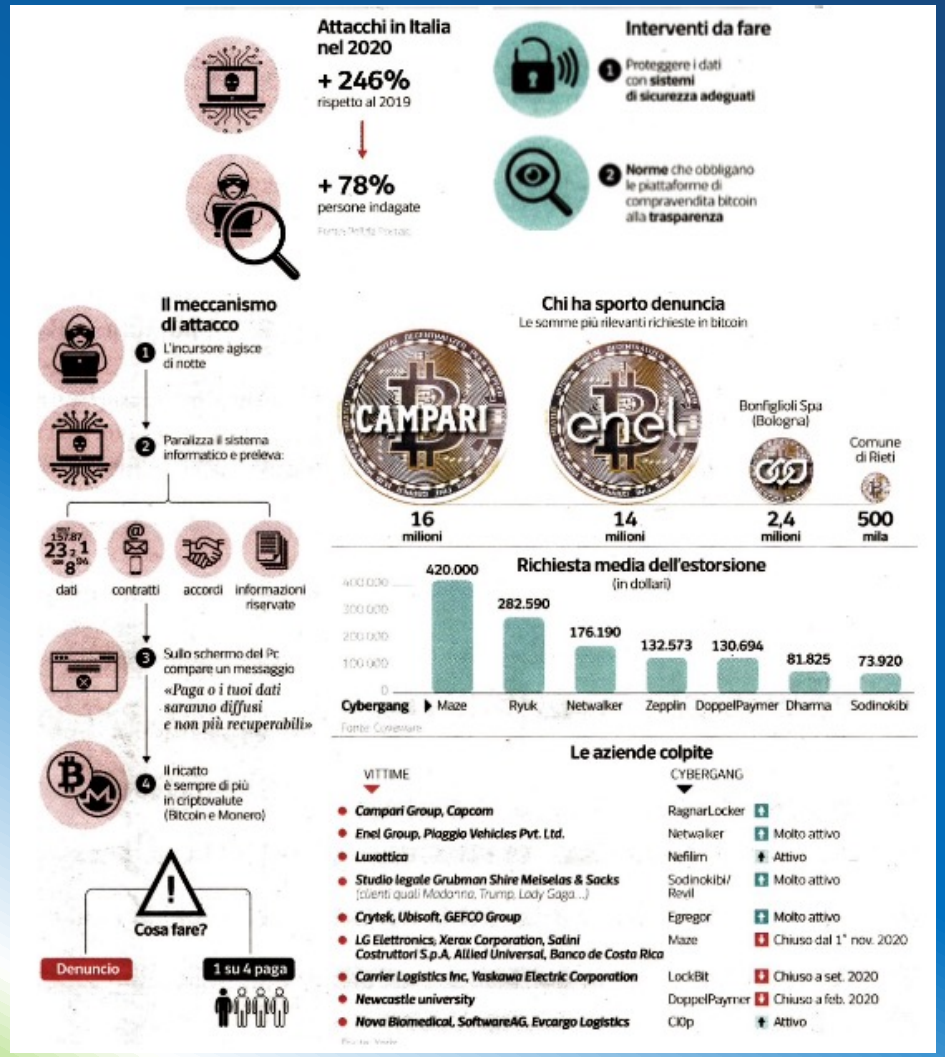
con il Patrocinio di:

A.I.PRO.S.
ASSOCIAZIONE ITALIANA
PROFESSIONISTI DELLA SICUREZZA

A.N.I.V.P.
ASSOCIAZIONE NAZIONALE
ISTITUTI DI VIGILANZA PRIVATA
E SERVIZI FIDUCIARI DI SICUREZZA

Phalanx MK2: Data Breach & Incident Response Management.

Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group



CORRIERE DELLA SERA | 15-FEB-2021 pagina 1-24

Cyberattacchi: +246% Un'azienda su 4 paga

NEL 2020 BOOM DI CRIMINI INFORMATICI: LA MAFIA DIGITALE RUBA I DATI DI ENTI E IMPRESE, POI CHIEDE IL RISCATTO IN CRIPTOVALUTA «MOLTI NON DENUNCIANO, TEMONO DANNI ALLA REPUTAZIONE»

IL RAPPORTO

Privacy, oltre 300 milioni di euro di sanzioni in Europa nel 2020

È quanto emerge dal rapporto dell'Osservatorio di Federprivacy in cui sono state analizzate le fonti istituzionali dello Spazio Economico Europeo (SEE).

di Nicola Bernardi*

CITEL Open-PSIM leadership
CyberLabs
con il Patrocinio di:
A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA
A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

Phalanx MK2: Data Breach & Incident Response Management.

Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group

Cyber crime: numero di breach e record esposti (in millioni), 2005-2019

Qual è il costo che un'azienda deve sostenere in caso di attacco hacker che comporti un data breach di queste dimensioni?

Una nota ricerca che risponde a questa domanda è quella svolta annualmente da Ponemon Institute, il "**2019 Cost of a Data Breach Report**", che quest'anno, sulla base di interviste a 500 organizzazioni medio grandi di tutto il mondo che hanno subito un data breach, stima che il costo medio per record sottratto sia pari a 150 dollari (era 145 dollari nel 2014). Per le aziende italiane che hanno partecipato allo studio il costo medio si attesta a un valore leggermente inferiore, **146 dollari per record sottratto**. L'analisi prende in considerazione un centinaio di fattori di costo potenziali, tecnologici, legali, regolatori, legati alla perdita del valore del brand, perdita di clienti e mancata produttività dei dipendenti.

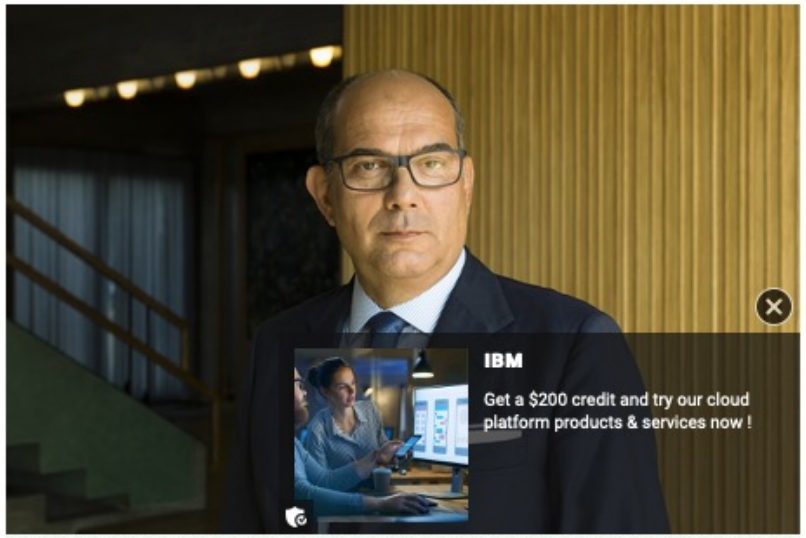
ANSA.it › Veneto › **Carraro: attacco hacker pesa su trimestre, ricavi -11%**

Carraro: attacco hacker pesa su trimestre, ricavi -11%

Esce ad Negri, guida passa a dg Conchetto

Redazione ANSA
MILANO
26 ottobre 2020
16:51
NEWS

Suggerisci
Facebook
Twitter
Altri
A+ A A-
Stampa
Scrivi alla redazione



- RIPRODUZIONE RISERVATA
CLICCA PER INGRANDIRE

CITEL Open-PSIM leadership
CyberLabs
con il Patrocinio di:
A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA
A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

Phalanx MK2: Data Breach & Incident Response Management.

Giovanni FINETTO – Vice-Presidente CyberLabs srl – Fondatore CyberTrust Group
Enrico MARCOLINI – Fondatore DOTTORMARC srl - Fondatore CyberTrust Group

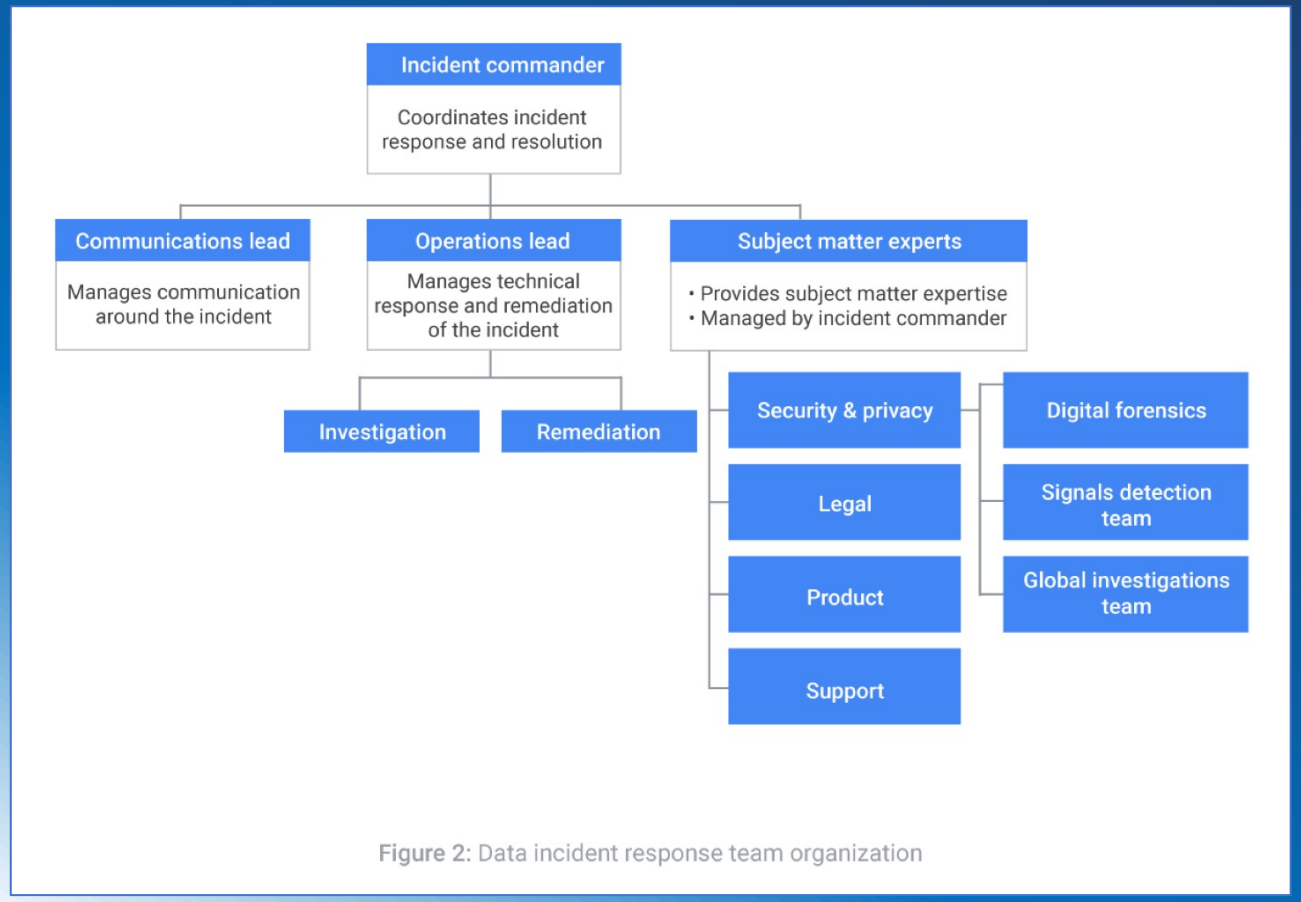


Figure 2: Data incident response team organization

CITEL Open-PSIM leadership
CyberLabs
con il Patrocinio di:
A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA
A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

L’importanza della formazione delle risorse aziendali per contrastare i rischi cyber: la cyber awareness.

Alfonso DE PAOLA – Amministratore Delegato CyberLabs srl

CITEL
Open-PSIM leadership

CyberLabs

con il Patrocinio di:

A.I.PRO.S.
ASSOCIAZIONE ITALIANA
PROFESSIONISTI DELLA SICUREZZA

A.N.I.V.P.
ASSOCIAZIONE NAZIONALE
ISTITUTI DI VIGILANZA PRIVATA
E SERVIZI FIDUCIARI DI SICUREZZA

L’importanza della formazione delle risorse aziendali per contrastare i rischi cyber: la cyber awareness.

Alfonso DE PAOLA – Amministratore Delegato CyberLabs srl

Articolo 32
EU RGPD
"Sicurezza del trattamento"

=> Motivo: 83, 74, 75, 76, 77
=> administrative fine: Art. 83 (4) lit a

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
=> Articolo: 24

a) la pseudonimizzazione e la cifratura dei dati personali;
=> Articolo: 4

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
=> Motivo: 75

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.
=> Articolo: 29

CITEL Open-PSIM leadership
CyberLabs
con il Patrocinio di:
A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA
A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

L’importanza della formazione delle risorse aziendali per contrastare i rischi cyber: la cyber awareness.

Alfonso DE PAOLA – Amministratore Delegato CyberLabs srl

degli attacchi informatici: a livello globale sono stati infatti **1.871 gli attacchi gravi di dominio pubblico** rilevati nel corso del 2020, ovvero con un impatto sistemico in ogni aspetto della società, della politica, dell’economia e della geopolitica. In termini percentuali, **nel 2020 l’incremento degli attacchi cyber a livello globale è stato pari al 12%** rispetto all’anno precedente; negli ultimi quattro anni il trend di crescita si è mantenuto pressoché costante, facendo segnare un aumento

Seguono le “tecniche sconosciute” (in riferimento alle quali prevalgono i casi di Data Breach, per il 20%), mentre **Phishing & Social Engineering** continuano ad essere la causa di una buona parte degli attacchi (15% del totale); si registra inoltre negli ultimi dodici mesi una crescita degli attacchi sferrati per mezzo di vulnerabilità note (+ 10%), precedentemente in calo (-29% nel 2019 rispetto al 2018).

Abbiano inoltre registrato nel corso degli ultimi dodici mesi un incremento di attacchi veicolati tramite l’abuso della **supply chain**, ovvero tramite la compromissione di terze parti, il che consente poi a criminali e spie di colpire i contatti (clienti, fornitori, partner) dell’obiettivo, ampliando notevolmente il numero delle vittime e passando più facilmente inosservati.

CITEL Open-PSIM leadership

CyberLabs

con il Patrocinio di:

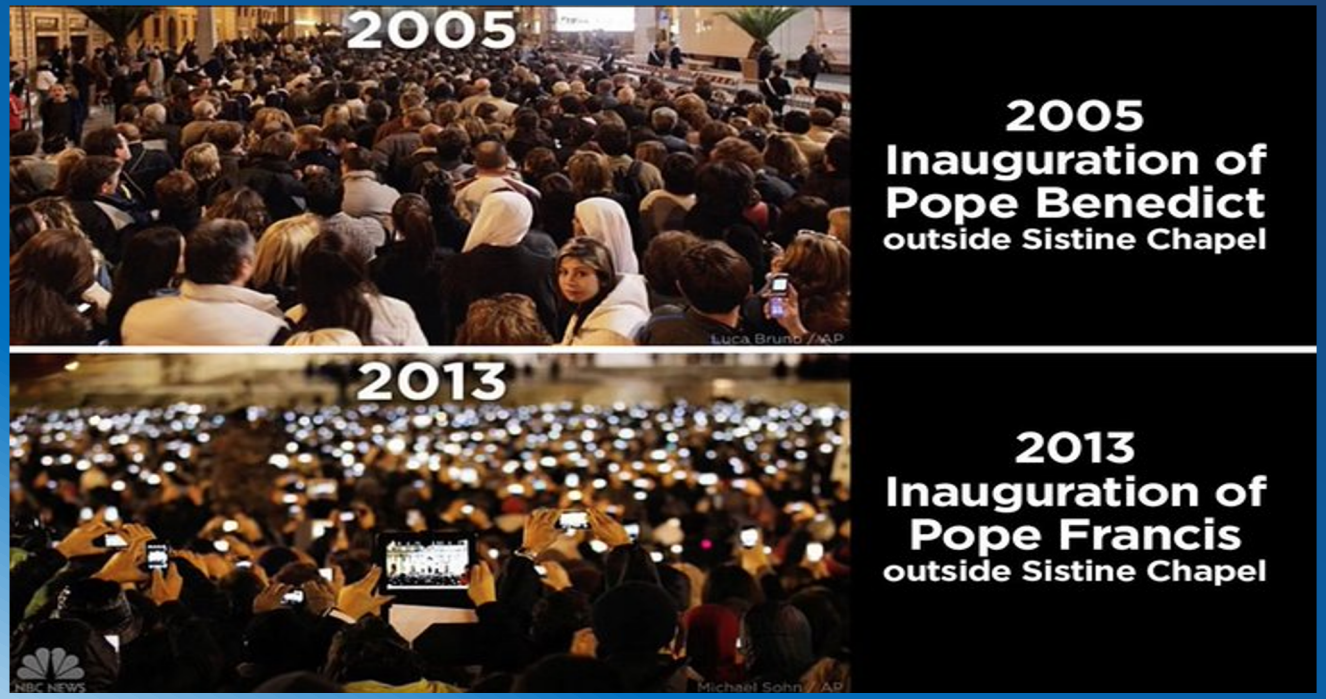
A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA

A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

L’importanza della formazione delle risorse aziendali per contrastare i rischi cyber: la cyber awareness.

Alfonso DE PAOLA – Amministratore Delegato CyberLabs srl

CYBERSECURITY E SMARTPHONE
Quanto è sicuro il tuo telefono?



AD UN CERTO PUNTO NELLA STORIA LE NOSTRE VITE SONO CAMBIATE…

CITEL Open-PSIM leadership
CyberLabs
con il Patrocinio di:
A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA
A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

L’importanza della formazione delle risorse aziendali per contrastare i rischi cyber: la cyber awareness.

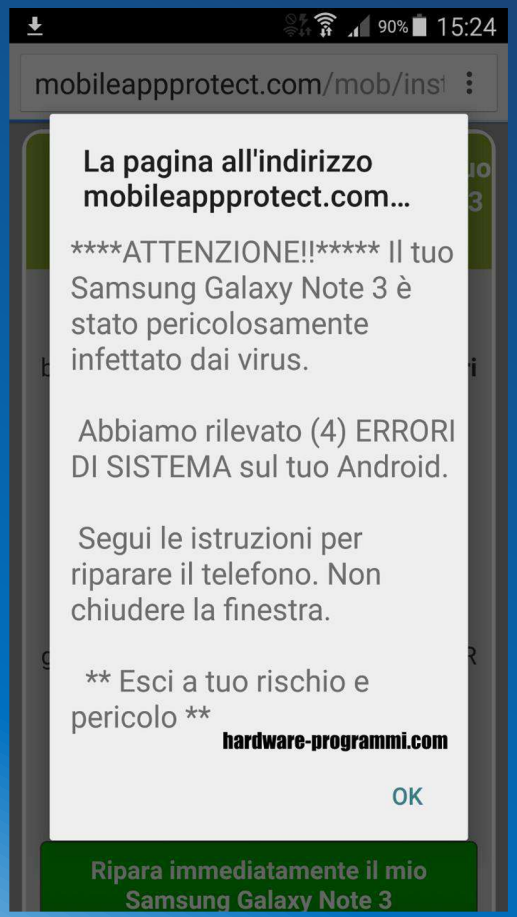
Alfonso DE PAOLA – Amministratore Delegato CyberLabs srl

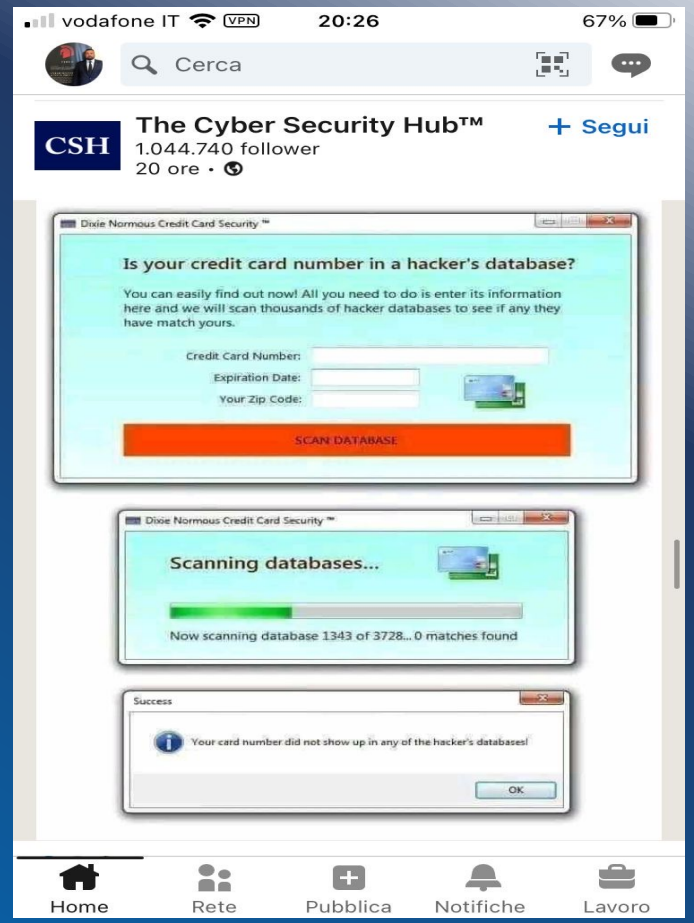
IDENTITÀ, PORTAFOGLIO, CHIAVI DI CASA E CODICI BANCARI: MOLTO PIÙ DI UN SEMPLICE TELEFONO

CITEL Open-PSIM leadership
CyberLabs
con il Patrocinio di:
A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA
A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

L’importanza della formazione delle risorse aziendali per contrastare i rischi cyber: la cyber awareness.

Alfonso DE PAOLA – Amministratore Delegato CyberLabs srl





CITEL Open-PSIM leadership

CyberLabs

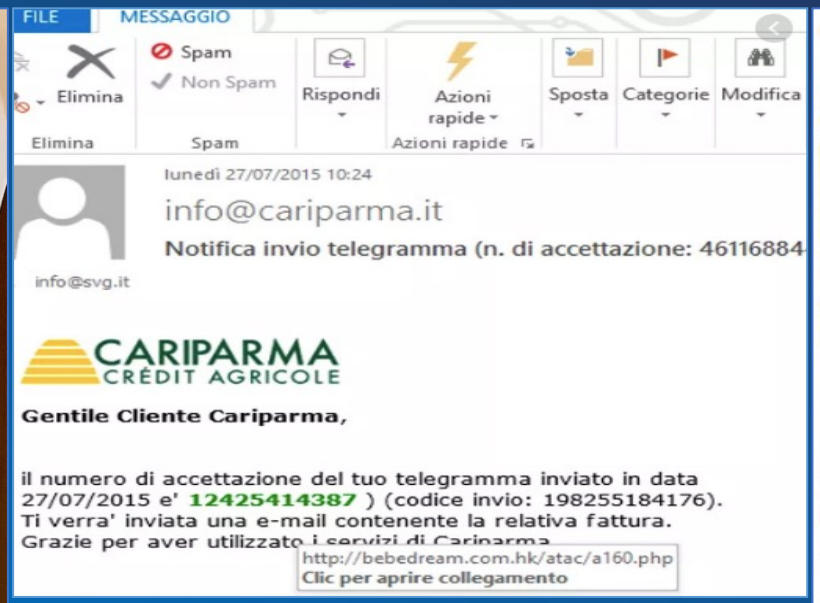
con il Patrocinio di:

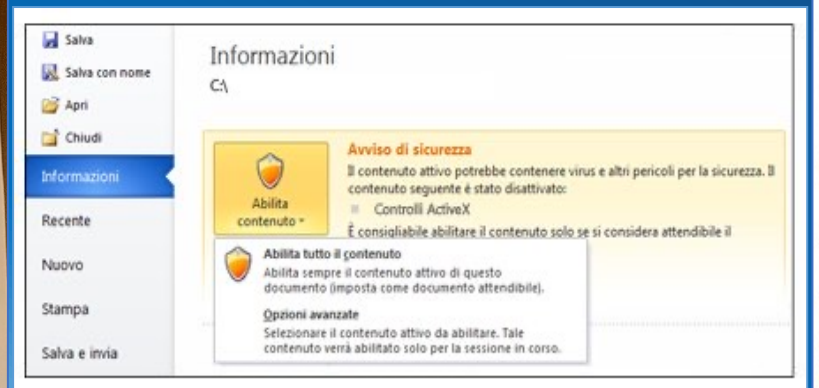
A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA

A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

L’importanza della formazione delle risorse aziendali per contrastare i rischi cyber: la cyber awareness.

Alfonso DE PAOLA – Amministratore Delegato CyberLabs srl





Telefona alla "banca" e dal conto gli spariscono 30mila euro

I carabinieri

18.09.2020

Riceve una telefonata dalla banca e dal suo conto spariscono 30mila euro. E' successo a un imprenditore vitivinicolo veronese che è stato raggirato con un attacco hacker chiamato "vishing".

CITEL Open-PSIM leadership

CyberLabs

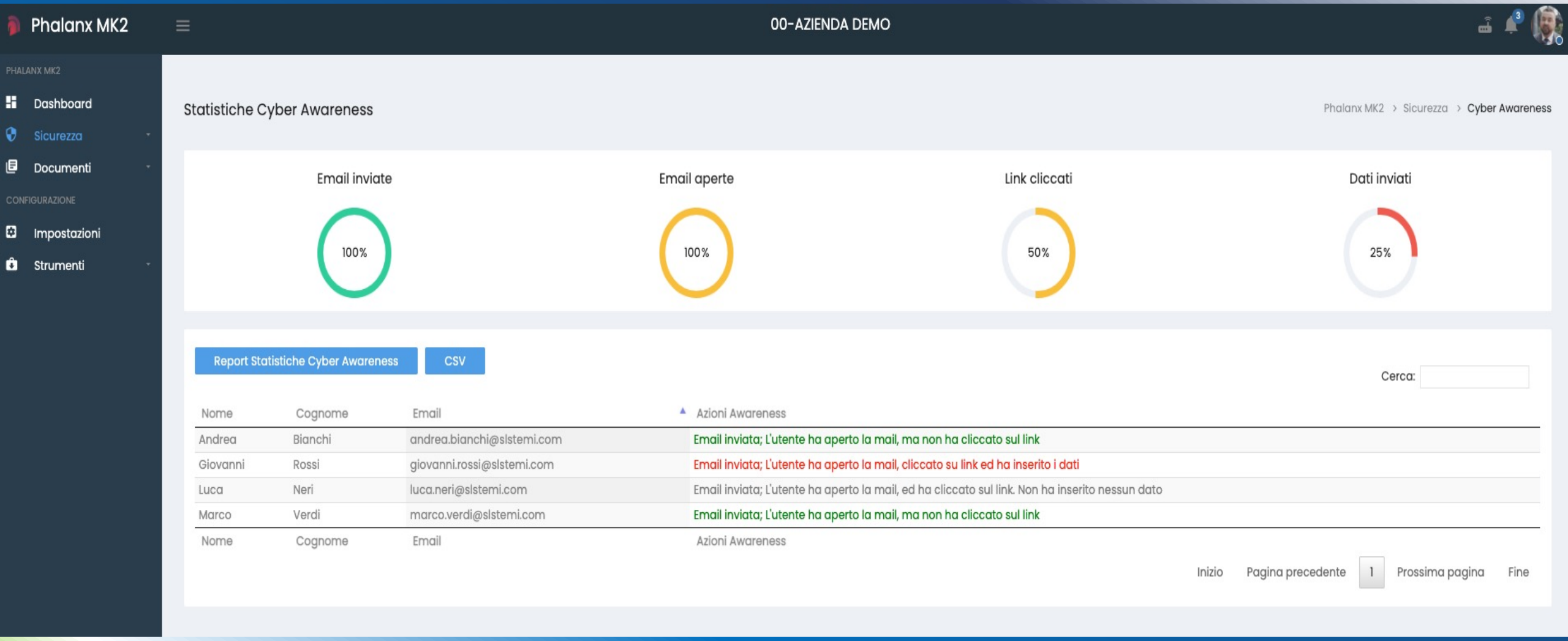
con il Patrocinio di:

A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA

A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

L’importanza della formazione delle risorse aziendali per contrastare i rischi cyber: la cyber awareness.

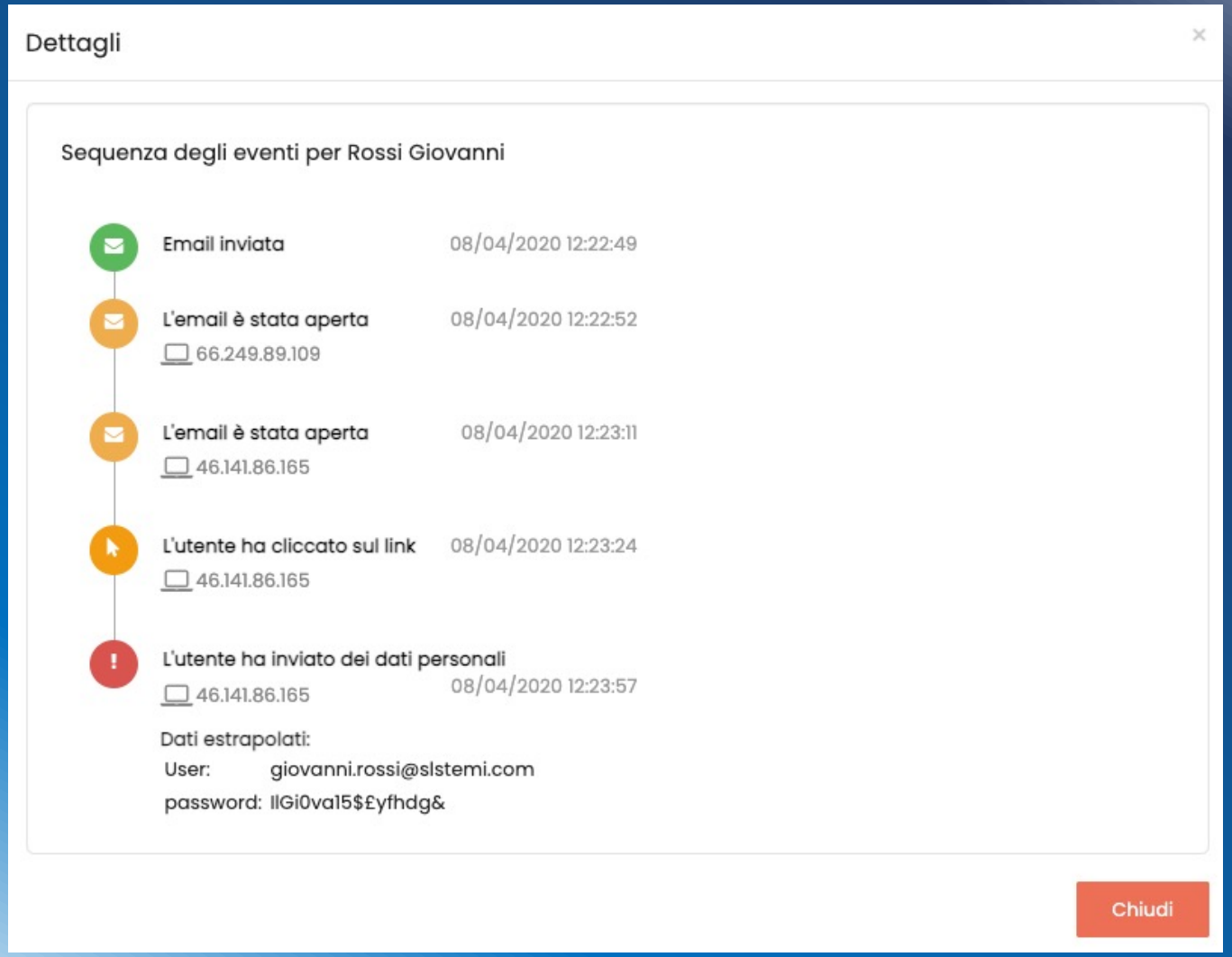
Alfonso DE PAOLA – Amministratore Delegato CyberLabs srl



CITEL Open-PSIM leadership
CyberLabs
con il Patrocinio di:
A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA
A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

L’importanza della formazione delle risorse aziendali per contrastare i rischi cyber: la cyber awareness.

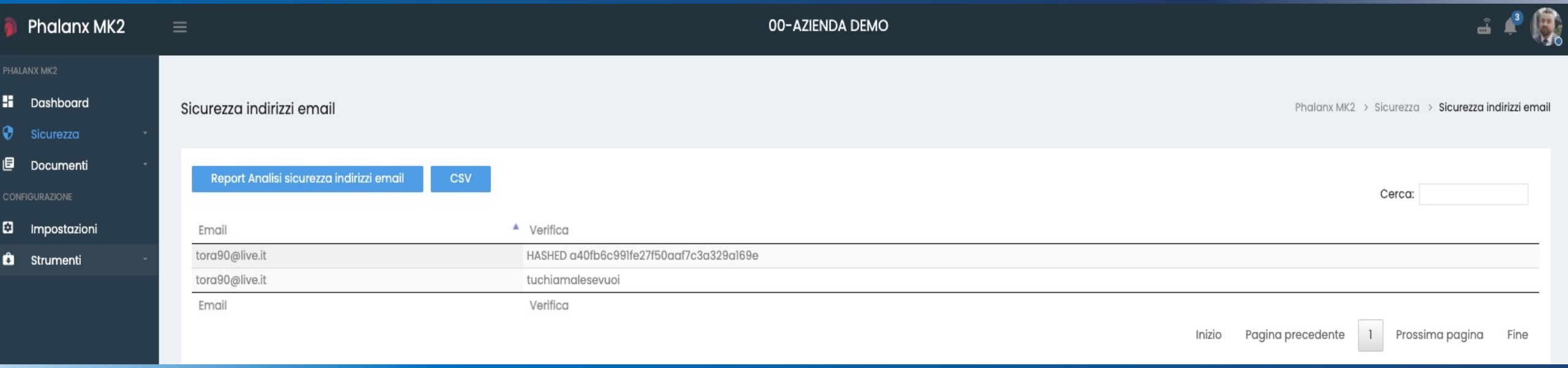
Alfonso DE PAOLA – Amministratore Delegato CyberLabs srl



CITEL Open-PSIM leadership
CyberLabs
con il Patrocinio di:
A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA
A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA

L’importanza della formazione delle risorse aziendali per contrastare i rischi cyber: la cyber awareness.

Alfonso DE PAOLA – Amministratore Delegato CyberLabs srl



CITEL Open-PSIM leadership

CyberLabs

con il Patrocinio di:

A.I.PRO.S. ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA

A.N.I.V.P. ASSOCIAZIONE NAZIONALE ISTITUTI DI VIGILANZA PRIVATA E SERVIZI FIDUCIARI DI SICUREZZA