SISTEMA BANCHE: MINACCE, PROTEZIONE, PREVENZIONE

Alessio Aceti

Head of Presales

AGENDA

INFORMAZIONI SULL'AZIENDA

Informazioni fondamentali

Fondata nel 1997 e guidata da Eugene Kaspersky

Holding registrata nel Regno Unito

Offre soluzioni di sicurezza IT innovative per aziende e privati

Numeri

Oltre 20 milioni di attivazioni di prodotti all'anno

711 milioni USD: ricavi globali non sottoposti a verifica del 2014

Oltre 3000 specialisti altamente qualificati

Risultati

Uno dei quattro principali fornitori di soluzioni per la sicurezza di endpoint*

"Leader" nel Gartner Magic Quadrant per le piattaforme di protezione di endpoint**

Le nostre soluzioni sono riconosciute e premiate in test e recensioni indipendenti

> 400.000.000

utenti in tutto il mondo scelgono i nostri prodotti di protezione

* La società ha conseguito il quarto posto nella classifica 2013 di IDC relativa ai fornitori nel settore della sicurezza degli endpoint con il maggior fatturato. La classifica è stata pubblicata nella relazione di IDC dal titolo "Worldwide Endpoint Security 2014–2018 Forecast and 2013 Vendor Shares" (IDC # 250210, agosto 2014). Nella relazione viene stilata una classifica di fornitori software basata sui ricavi ottenuti dalla vendita di soluzioni per la sicurezza degli endpoint nel 2013.

**Gartner, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, John Girard, Neil MacDonald, 8 gennaio 2014. La relazione è disponibile presso Kaspersky Lab su richiesta.

AREE GEOGRAFICHE

200 paesi
e territori
in cui operiamo

35 uffici regionali
di rappresentanza

Nord America
Canada
Messico
Stati Uniti

Sud America
Brasile

Europa
Austria
Danimarca
Francia
Germania
Israele
Italia
Paesi Bassi
Polonia
Portogallo
Regno Unito
Romania
Russia
Spagna
Svizzera
Ucraina

Asia
Cina
EAU
Giappone
Hong Kong
India
Kazakhstan
Malesia
Singapore
Sud Corea
Turchia

Africa
Sudafrica

Australia

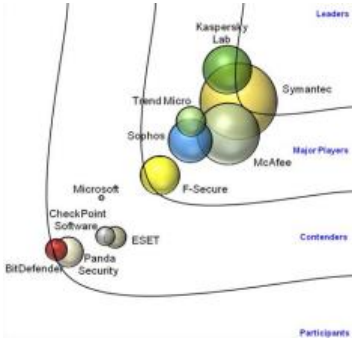
KASPERSKY LAB È MARKET LEADER

Gartner

2014. A Leader. Magic Quadrant for Endpoint Protection Platform*

FORRESTER®

A leader in the Forrester Wave for Endpoint Security, The Forrester Wave™: Endpoint Security, Q1 2013**



IDC

Leader in IDC MarketScape***

* Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.
** The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.
*** IDC's Go-to-Market Services (GMS) offers webrights and reprints of IDC research to support your marketing initiatives. GMS can also help you to leverage IDC's globally respected brand by delivering custom content and multimedia deliverables which are drawn from research and analysis independently conducted and published by IDC analysts. Learn more here or contact us at gms@idc.com

KASPERSKY lab

SOCIAL ENGINEERING E AWARENESS

BASTANO DEGLI STRUMENTI FISICI O INFORMATICI?

L’**80%**degli incidenti di sicurezza IT è causato da errori umani.

Un educazione dedicata al personale non-IT può diminuire il numero di incidenti del **90%**

Gartner 2014: Organizations are seeking more sophisticated behavioral support approaches (for example, corporate culture development) that support continued investment in awareness and security education.

SOCIAL ENGINEERING PENETRATION TEST

Siete certi che il Vostro personale sia in grado di riconoscere un attacco di social engineering?

Identificare i rischi

Identificare il target

Simulare un attacco

Analizzare i risultati

Remediation

PHYSICAL PENETRATION TEST

Chi lavora nelle sedi periferiche conosce le procedure? Ne conosce l’importanza? Le applica nel lavoro quotidiano?

Identificare i rischi

Identificare i target

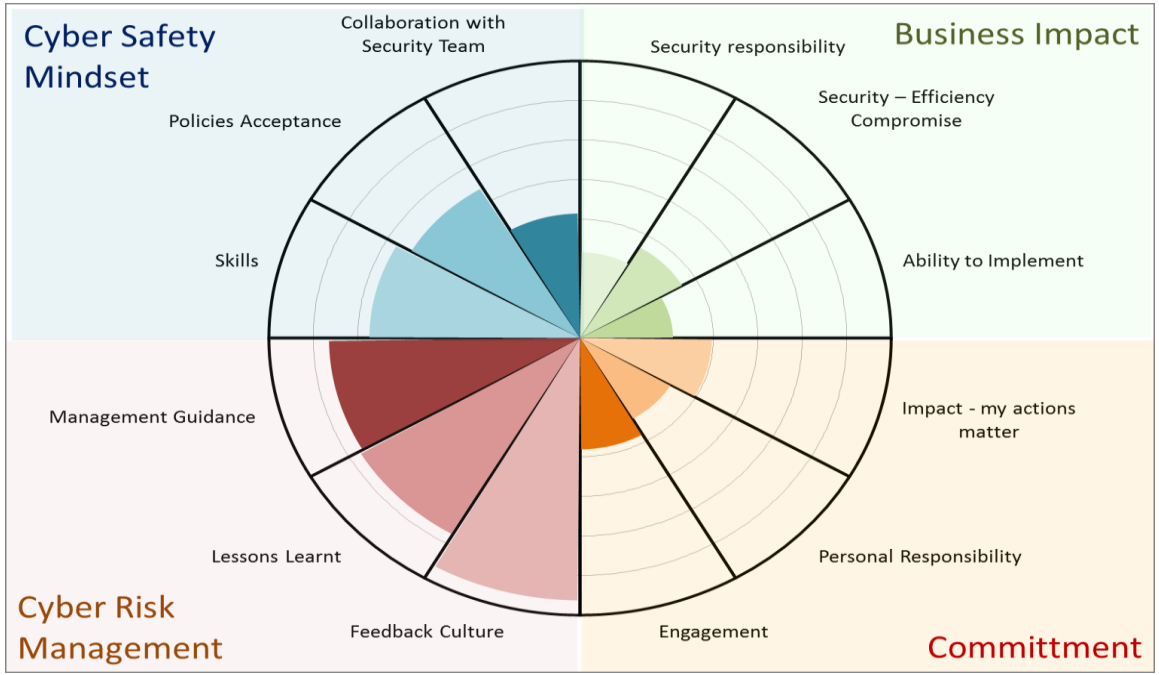
Simulare un attacco

Analizzare i risultati

Remediation

CYBER SAFETY CULTURE ASSESSMENT

Come identificare quali sono i gap ?

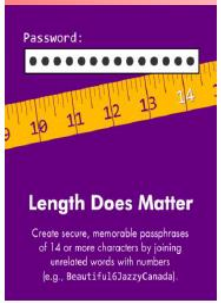


COME PREVENIRE?

LO SCENARIO

- L’80% degli incidenti di sicurezza informatica è causata da errori umani
- Educare i dipendenti può diminuire questi incidenti del 90%
- La Cybersecurity awareness è l’elemento «must have» della sicurezza informatica
- Forse state già spendendo denaro per questo tipo di formazione ma...

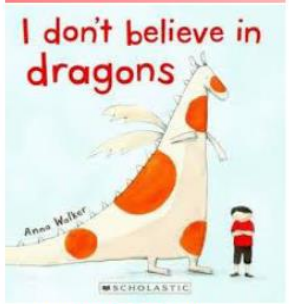
Posters are not enough



Boring frustrating Trainings

Too long
Too technical
Too skeptical (only treats and “Don’t”, without “DOs”)

No motivation, wrong beliefs

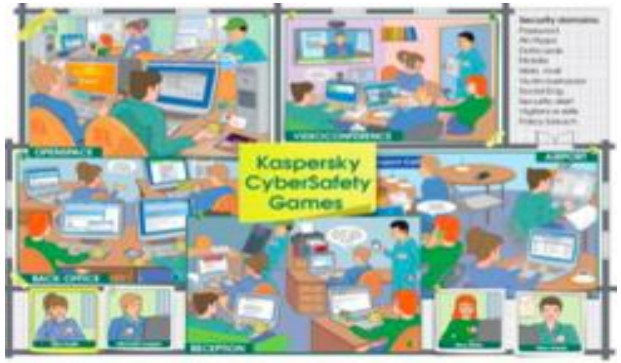


Only 22% believe they can be targeted by cybercriminals.

Employee do not see IT Security as partners

TRAINING PROGRAM

CyberSafety: Onsite



- Gioco interattivo a squadre che affronta 9 temi di cybersecurity.
- Impersonare il Cybercriminiale, giocare in squadra per aumentare la security awarness.
- Almeno10% dello staff

CyberSafety: Online

- Training Online che affronta 11 temi diversi di cybersecurity
- Analisi delle competenze raggiunte
- Materiale sulla Sicurezza informatica fornito a supporto (posters, email templates, screensaver)

KASPERSKY lab

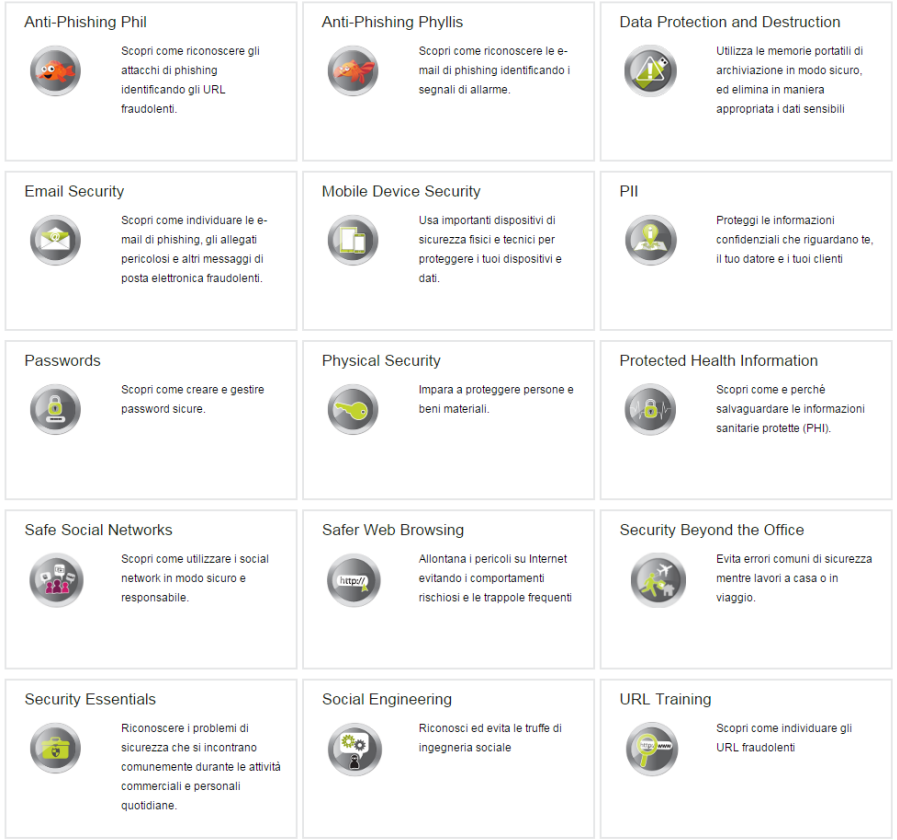
ONLINE TRAINING PLATFORM

Vengono assegnati brevi moduli di formazione.

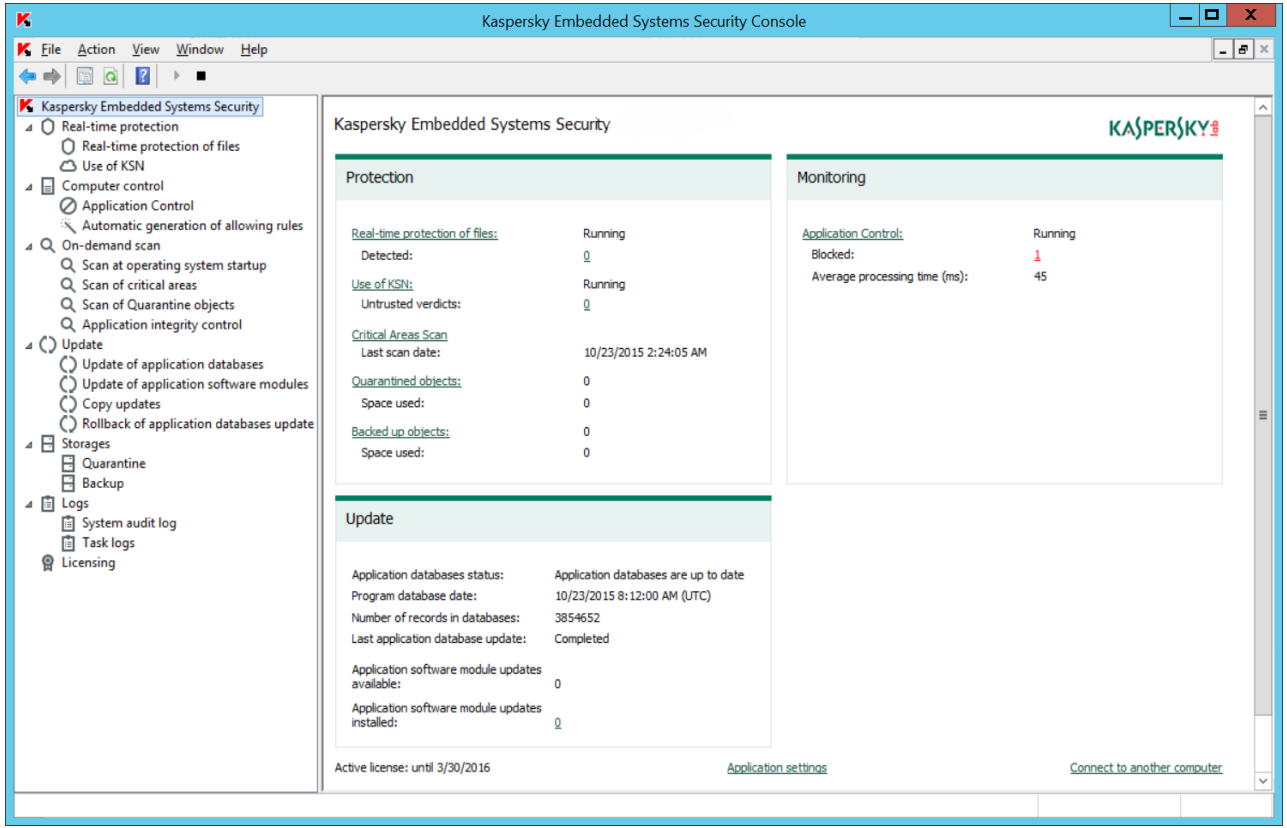
L’amministratore può vedere e gestire i vari progressi dei singoli utenti.

Invio di mail «fake» per testare la reazione dei singoli utenti.

Reportistica personalizzata.



COMING SOON



KASPERSKY lab

DOMANDE?

KASPERSKY lab