Sec-lab.com

4 Febbraio 2021

Cyber Security: un approccio multidimensionale

Introduzione di Alberto Redi : Partner & CEO Security Lab Group

securitylab
CYBER SECURITY

Cyber Security: un approccio multidimensionale

WEBINAR 2021

Governance & Compliance

Infrastrutture

Applicazioni

Risorse umane

4	febbraio 2021	**Perimetro di applicazione della Cyber Security**
11	febbraio 2021	**Governance della Cyber Security e Compliance alle normative**

securitylab
CYBER SECURITY

Sec-lab.com

4 Febbraio 2021

Intelligenza Artificiale e Machine Learning al servizio della Cyber Security

Infrastrutture

Sommario / Relatori

Andrea Palanca

Senior Cyber Security Advisor **Security Lab**

- L'evoluzione dei sistemi di protezione delle infrastrutture ICT
- Darktrace: simulazione di attacco reale rilevato

Jacopo Maria Tavaroli

Senior Cyber Security Advisor **iQuasar**

- La protezione tramite intelligenza artificiale e machine learning
- Darktrace: demo dell'interfaccia grafica

Stefania Siro

Account Executive
Darktrace Italia

Mariana Pereira

Country Manager
Darktrace Italia

Leonardo Ruvitoso

Cyber Technology Specialist
Darktrace Italia

2020 Principali tendenze e nuove minacce Cyber: incidenti reali rilevati con AI & ML

Leonardo Cappabianca

Cyber Technology Specialist
Darktrace Italia

AI e ML a protezione dei sistemi industriali

securitylab
CYBER SECURITY

Sec-lab.com

4 Febbraio 2021

Infrastrutture

L'evoluzione dei sistemi di protezione delle infrastrutture ICT

Andrea Palanca : Senior Cyber Security Advisor Security Lab

L'evoluzione dei sistemi di protezione delle infrastrutture ICT

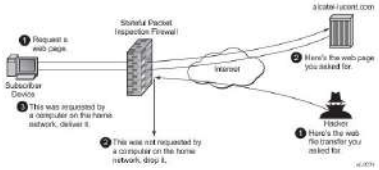
Con l'introduzione delle reti LAN nella seconda metà degli anni 1970 e l'aumentare della connettività tra queste, cominciarono a emergere i primi problemi di sicurezza riguardanti gli accessi non autorizzati ad una rete.

Una delle prime soluzioni adottate consisteva nell'impostare all'interno dei router le liste di controllo degli accessi (ACL) che consentivano di stabilire quali pacchetti accettare e quali scartare sulla base dell'indirizzo IP. Questo approccio diventò sempre meno utilizzabile quanto più aumentavano gli host connessi alla rete Internet.

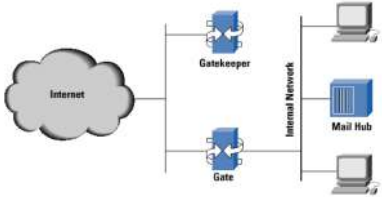
Per cercare di contrastare le intrusioni, alla fine degli anni 1980 iniziarono a diffondersi i primi sistemi di sicurezza, su due fronti: i firewall, per la sicurezza delle reti, e gli antivirus, per la sicurezza dei dispositivi in esse presenti.

L'evoluzione dei sistemi di protezione delle infrastrutture ICT

Stateless Packet Filter Firewall
Filtraggio sulla sola base dell'header dei pacchetti.
Potevano essere facilmente aggirati utilizzando l'IP spoofing.



Stateful Packet Filter Firewall
Filtraggio basato sugli header e sullo stato delle connessioni.
Gli attacchi di tipo IP spoofing venivano mitigati, tuttavia ancora non garantivano la protezione da attacchi nei livelli superiori del modello OSI, requisito sempre più importante a causa degli attacchi alle applicazioni web sempre più frequenti.

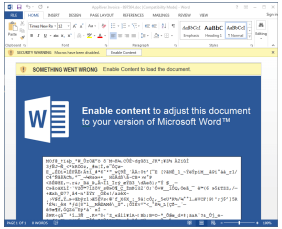


Application Firewall
Firewall di nuova generazione in grado di offrire protezione fino al livello applicativo (livello 7) del modello OSI.

L'evoluzione dei sistemi di protezione delle infrastrutture ICT

Antivirus (inizi)
Identificazione di file sulla sola base delle firme di virus noti.
Richiedevano costanti difficoltosi aggiornamenti (spesso distribuiti via floppy disk) ed erano facilmente aggirabili con lievi modifiche al codice del virus.

Antivirus (anni 90-2000)
Riconoscimento di sempre più tipologie di minacce (allegati via mail, pagine aperte via browser, rootkit, ecc.) e debutto delle prime soluzioni basate su motori «euristici», in grado di identificare i software malevoli solo sulla base del loro comportamento.



Antivirus (oggi)
Approcci completamente «signature-less», che includono l'uso di behavioral detection, artificial intelligence, machine learning e cloud-based file detonation allo scopo di incrementare sempre di più il rilevamento di minacce 0-day.

L'evoluzione dei sistemi di protezione delle infrastrutture ICT

Seppure i sistemi di sicurezza prima menzionati abbiano fatto notevoli passi avanti dal loro debutto ad oggi, alcuni problemi rimangono ancora aperti:

- Come identifichiamo un evento di data exfiltration, che non consiste nell'esecuzione di malware oppure exploit applicativi (per esempio, il caso del dipendente infedele)?
- Come possiamo rilevare un dispositivo compromesso (per esempio, un dispositivo IoT) oppure un nuovo dispositivo estraneo aggiunto sulla rete?
- Come possiamo investigare un'attività sospetta passata, per determinare se c'è stato un data breach?

securitylab
CYBER SECURITY

Sec-lab.com

4 Febbraio 2021

Infrastrutture

La protezione tramite Intelligenza Artificiale e Machine Learning

Jacopo Maria Tavaroli : Senior Cyber Security Advisor iQuasar
Andrea Palanca : Senior Cyber Security Advisor Security Lab

La protezione tramite Intelligenza Artificiale e Machine Learning

Se soluzioni basate su regole e firme offrono una qualche protezione contro minacce pre-identificate, la realtà è che gli attacchi eludono continuamente queste soluzioni e ottengono l'accesso alla rete.

Darktrace, alimentata da un machine learning "unsupervised", risponde a queste minacce prima che si trasformino in crisi.

L'applicazione di intelligenza artificiale alle sfide di cyber defense ha segnato un cambiamento fondamentale nella nostra capacità di proteggere i sistemi di dati e le infrastrutture digitali fondamentali.

Ai team della sicurezza sotto stress offre la possibilità di rimanere al passo con il panorama delle minacce in continua evoluzione.

La protezione tramite Intelligenza Artificiale e Machine Learning

La **cyber IA** è tecnologia di auto-apprendimento che, come il sistema immunitario dell'uomo, apprende "in corsa d'opera" dai dati e dalle attività che osserva in situ. Ciò significa fare miliardi di calcoli basati sulla probabilità alla luce di evidenze in continua evoluzione.

Questa capacità di auto-apprendimento consente alla cyber IA di scoprire pattern rari e precedentemente mai visti, tra il caos dell'attività quotidiana, all'interno dei sistemi digitali di un'organizzazione. Rilevando lievi deviazioni dal "pattern of life" dell'organizzazione, è in grado di distinguere gli amici dai nemici ed evidenziare minacce o attacchi informatici reali che altrimenti non sarebbero notati.

Poiché sta emergendo una nuova generazione di minacce informatiche, alimentata da IA offensiva, la risposta indipendente guidata dall'IA sarà fondamentale per reagire con la precisione e la velocità necessarie. Questi attacchi alla velocità delle macchine saranno contrastati solo da difese guidate dall'IA, che potranno essere un passo avanti, consentendo alle persone di avere tempo prezioso per aggiornarsi.

La protezione tramite Intelligenza Artificiale e Machine Learning

Le tecnologie principali di Darktrace sono tre:

- **Enterprise Immune System**
- **Darktrace Antigena**
- **Cyber AI Analyst**

La protezione tramite Intelligenza Artificiale e Machine Learning

*L'**Enterprise Immune System** è una tecnologia IA di auto-apprendimento che rileva nuovi attacchi e minacce interne nella loro fase iniziale.*

L'Enterprise Immune System utilizza un machine learning "unsupervised" e l'IA per comprendere tutto ciò che riguarda l'organizzazione. Osservando gli utenti e i dispositivi, i cloud container e i flussi di lavoro, apprende "in corso d'opera" tutto ciò che è normale per l'organizzazione.

Diversamente dagli approcci tradizionali che fanno affidamento su blacklist, regole e firme, l'approccio "immune system" apprende dai dati, creando una comprensione su misura e in evoluzione degli ambienti digitali. Questo approccio esclusivo consente a Darktrace di rilevare le minacce informatiche più sofisticate e furtive che altri strumenti non sono in grado di rilevare.

Indipendentemente da una nuova specie di ransomware o un attacco interno emergente, l'Enterprise Immune System rileva la minaccia nelle primissime fasi.

La protezione tramite Intelligenza Artificiale e Machine Learning

***Darktrace Antigena** è la prima soluzione al mondo di Risposta autonoma.*

Darktrace Antigena entra in azione contro le minacce informatiche in corso, arrestandone il percorso prima che si verifichi qualsiasi danno. Fondamentale per la difesa contro minacce in rapido movimento come i ransomware, Antigena reagisce in pochi secondi, dando al team della sicurezza il tempo di attivarsi senza interrompere le operazioni aziendali quotidiane.

Le sue decisioni autonome sono:

- prese in tempo reale
- aggiornate ripetutamente attraverso l'osservazione continua delle minacce non appena si diffondono
- informate da comportamenti combinati, non da singoli punti di dati
- basate su un'ampia comprensione di dispositivi e persone all'interno dell'organizzazione

La protezione tramite Intelligenza Artificiale e Machine Learning

***Cyber AI Analyst** è una tecnologia che sfrutta la migliore esperienza degli analisti della sicurezza di prim'ordine per automatizzare maggiormente il processo di indagine e incrementare l'analisi della sicurezza.*

Imparando da un ampio set di dati creato da migliaia di implementazioni IA in tutto il mondo, la tecnologia esegue un'indagine qualificata alla velocità delle macchine, garantendo un significativo risparmio di tempo per l'analisi della sicurezza.

Cyber AI Analyst è in grado di correlare intelligentemente punti dati eterogenei all'interno del business digitale, aiutando i team della sicurezza a indagare più velocemente e in modo più efficace sulle minacce.

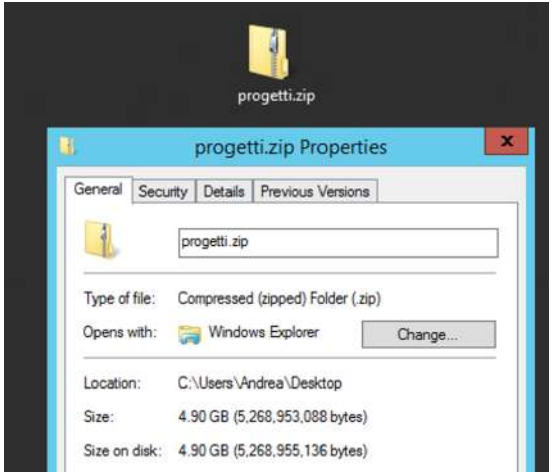
Cyber AI Analyst conduce indagini approfondite prima che qualsiasi cosa sia portata all'attenzione dei team umani della sicurezza, consente di scartare gli eventi a bassa priorità o innocui fin dall'inizio, nonché di presentare in qualsiasi momento solo pochi incidenti ad alta priorità.

La protezione tramite Intelligenza Artificiale e Machine Learning

La protezione tramite Intelligenza Artificiale e Machine Learning

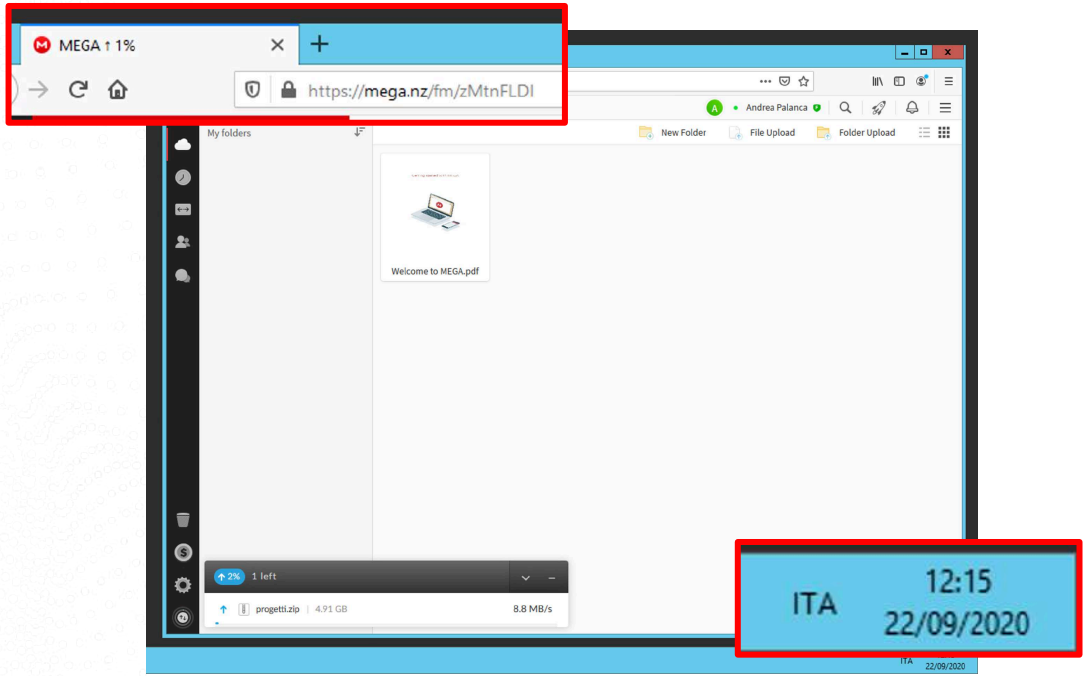
Come identifichiamo un evento di data exfiltration, che non consiste nell'esecuzione di malware oppure exploit applicativi (per esempio, il caso del dipendente infedele)?

Simulazione di data exfiltration: upload su Mega.nz di una cartella compressa di progetti aziendali



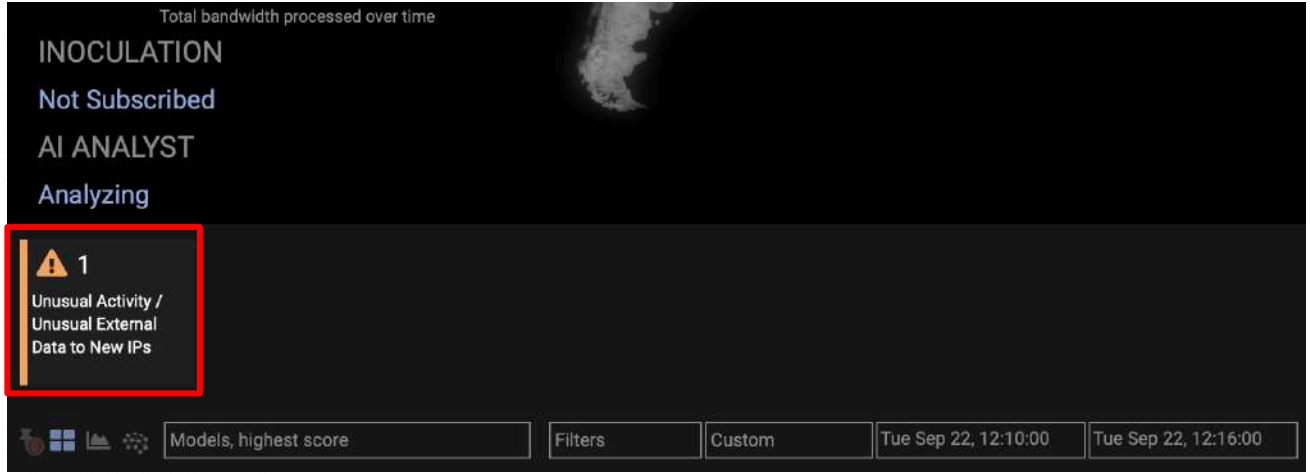
La protezione tramite Intelligenza Artificiale e Machine Learning

Simulazione di data exfiltration: upload su Mega.nz di una cartella compressa di progetti aziendali



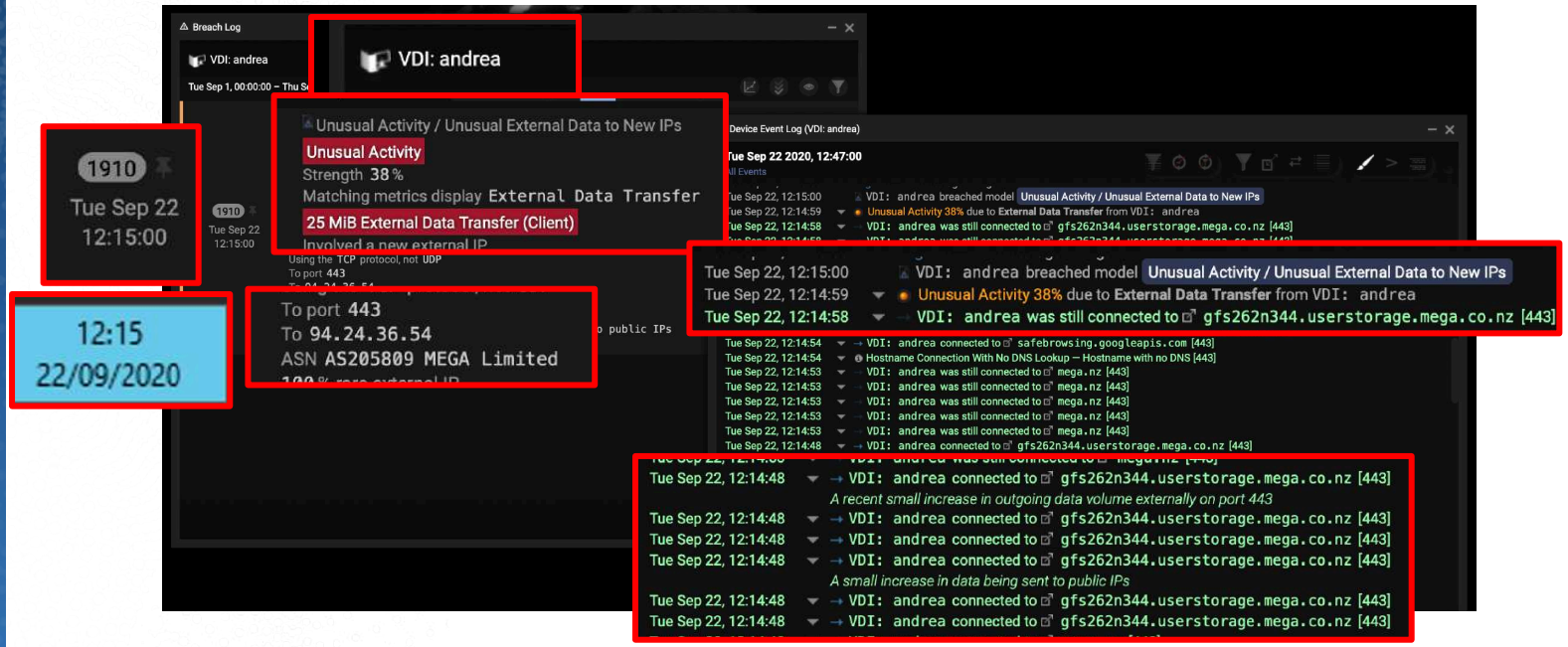
La protezione tramite Intelligenza Artificiale e Machine Learning

Simulazione di data exfiltration: upload su Mega.nz di una cartella compressa di progetti aziendali



La protezione tramite Intelligenza Artificiale e Machine Learning

Simulazione di data exfiltration: upload su Mega.nz di una cartella compressa di progetti aziendali



securitylab
CYBER SECURITY

Sec-lab.com

4 Febbraio 2021

Infrastrutture

2020 Principali tendenze e nuove minacce Cyber: incidenti reali rilevati con AI & ML

Stefania Siro: Account Executive Darktrace IT
Mariana Pereira : Director e-Mail Security Products Darktrace UK
Leonardo Ruvitoso : Cyber Technology Specialist Darktrace IT

securitylab
CYBER SECURITY

Sec-lab.com

4 Febbraio 2021

Infrastrutture

AI & ML per la protezione dei sistemi industriali

Leonardo Cappabianca: Cyber Technology Specialist Darktrace IT

Cyber Defence Center Ticino

Il team di Security Lab offre servizi di SOC di nuova generazione, non invasivi e con minime complessità progettuali utilizzando tecnologia Darktrace

- L'implementazione delle sonde Darktrace richiede qualche ora di lavoro
- Le sonde Darktrace non sono invasive e necessitano soltanto della copia del traffico di rete in modalità passiva
- E' possibile testare gratuitamente la tecnologia Darktrace per un mese, con il coordinamento di Security Lab per tutta la durata della POV (Proof of Value)
- Security Lab offre un servizio di monitoraggio dei rilievi e incidenti di Darktrace, eseguendo il primo «triage» degli allarmi, in modo da coinvolgere il personale aziendale solo quando necessario
- Vengono offerti dei report periodici degli allarmi
- I dati sul traffico rilevato da Darktrace non escono dalla azienda e in nessun modo vengono trasferiti fuori dal territorio della Confederazione

securitylab
CYBER SECURITY

Sec-lab.com

4 Febbraio 2021

Metodi di attacco alle applicazioni web e formazione Web Application Hacking

Applicazioni

Sommario / Relatori

Andrea Costantino
Senior Cyber Security Advisor **Security Lab**

Facundo Pantaleo
Senior Cyber Security Advisor **Security Lab**

- Tecniche di attacco alle Web Application: Hacking Live
- Nuovissimo Corso Web Application Hacking

securitylab
CYBER SECURITY

Sec-lab.com

4 Febbraio 2021

Applicazioni

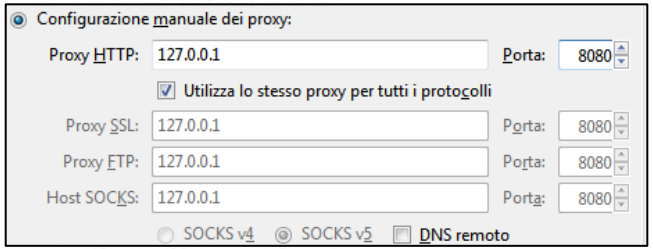
Tecniche di attacco alle Web Application: Hacking Live

Facundo Pantaleo: Senior Cyber Security Advisor Security Lab
Andrea Costantino:Senior Cyber Security Advisor Security Lab

Burp Suite

- Software utilizzato per effettuare penetration test sulle applicazioni web.
- I principali componenti di Burp Suite sono: **Proxy,** Intruder, **Repeater** e Sequencer.
- **Proxy**: permette di ispezionare e modificare il traffico. Si interpone fra il browser e l'applicazione da analizzare.
- **Repeater**: manipola e ri-invia il contenuto di una richiesta.

MySQL
CSS3
HTML5
PHP
XHTML
ERP
CRM
WP
Web Applications


Configurazione manuale dei proxy:
Proxy HTTP: 127.0.0.1
Porta: 8080
Utilizza lo stesso proxy per tutti i protocolli
Proxy SSL: 127.0.0.1
Porta: 8080
Proxy FTP: 127.0.0.1
Porta: 8080
Host SOCKS: 127.0.0.1
Porta: 8080
SOCKS v4
SOCKS v5
DNS remoto

Broken Access Control

- La maggior parte dei sistemi informatici è progettata per essere utilizzata con più utenti. Ogni utente ha dei privilegi che lo autorizzano ad un serie di azioni come la visualizzazione e la modifica dei file.

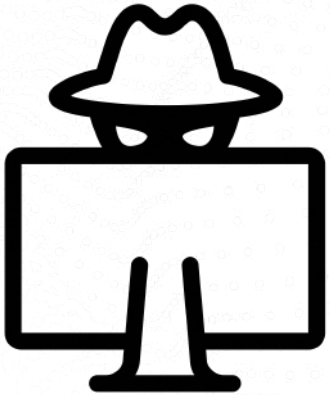
- Si parla di ''privilege escalation'' quando un utente riceve i privilegi a cui non ha diritto. Questi privilegi possono essere utilizzati per eliminare file, visualizzare informazioni private o installare programmi indesiderati come i virus.

- La ''privilege escalation'' avviene in due forme:

  - **Verticale**: un utente con privilegi inferiori accede a funzioni o contenuti riservati a utenti con privilegi superiori.

  - **Orizzontale**: un utente normale accede a funzioni o contenuti riservati ad altri utenti normali.

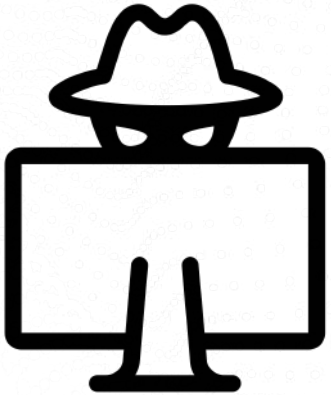
Broken Access Control



GET /basket/id/1

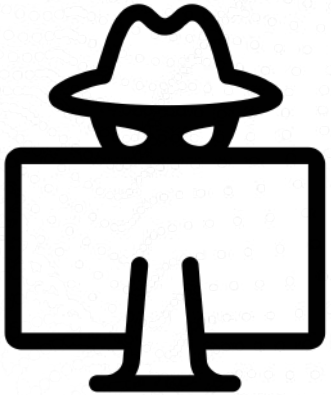
Broken Access Control

Broken Access Control



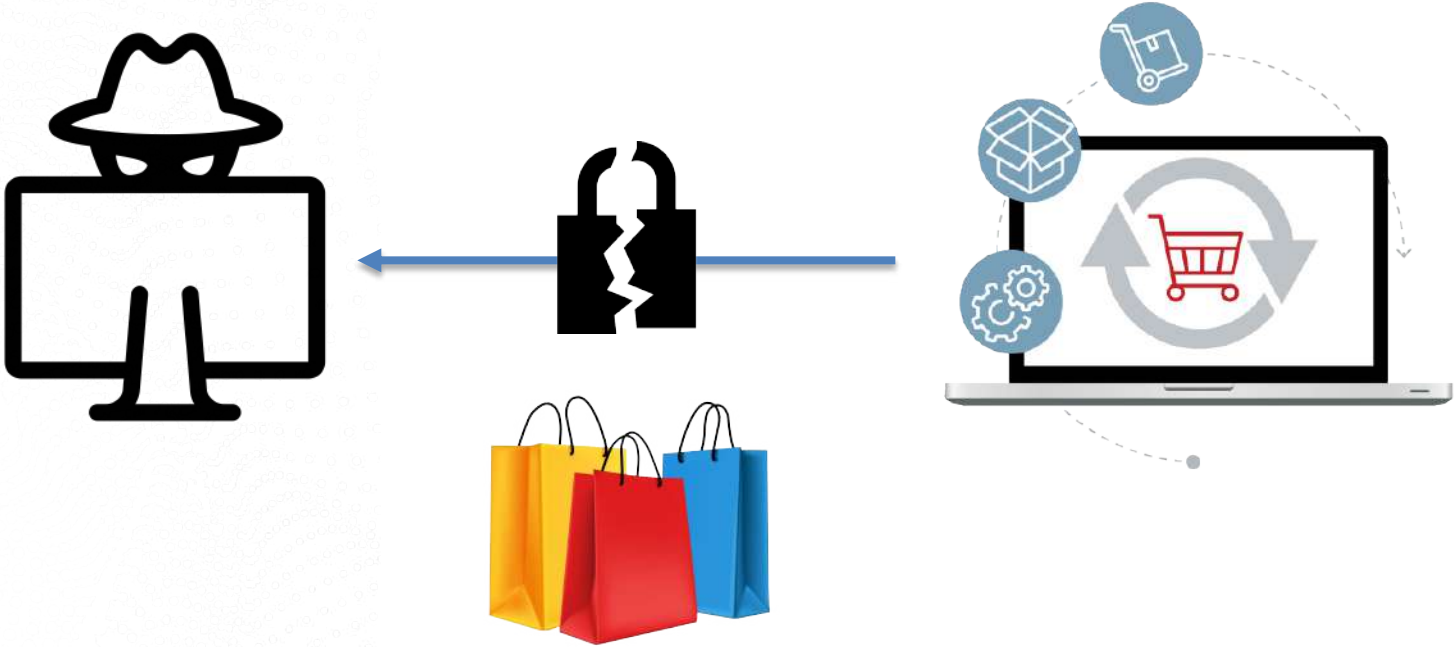
GET /basket/id/

Broken Access Control



GET /basket/id/**X**

Broken Access Control

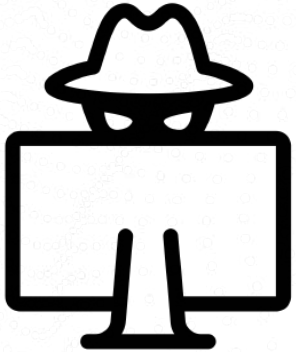


Improper Input Validation

- La validazione dell’Input è una tecnica utilizzata per controllare input potenzialmente pericolosi al fine di garantire che gli input siano elaborati in modo sicuro all'interno del codice o durante la comunicazione con altri componenti.

- Quando il software non convalida correttamente l'input, un attaccante è in grado di creare l'input in una forma che non è prevista dal resto dell'applicazione. Ciò porterà parti del sistema a ricevere input non intenzionali, il che potrebbe comportare un flusso alterato, un controllo arbitrario di una risorsa o l'esecuzione di codice arbitrario.

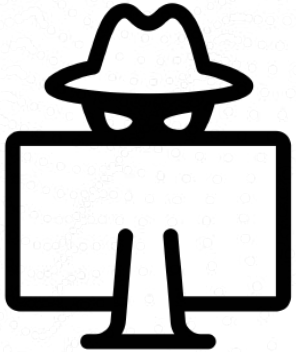
Improper Input Validation



customer


```
{
  "email":"test@visionary.day",
  "password":"12345",
  "passwordRepeat":"12345",
  "securityQuestion":{
    "id":1,
    "question":"Your eldest siblings middle name?",
    "createdAt":"2020-09-30T15:04:31.533Z",
    "updatedAt":"2020-09-30T15:04:31.533Z"
  },
  "securityAnswer":"a"
}
```

Improper Input Validation



admin


```
{
  "email":"test@visionary.day",
  "password":"12345",
  "passwordRepeat":"12345",
  "role":"admin",
  "securityQuestion":{
    "id":1,
    "question":"Your eldest siblings middle name?",
    "createdAt":"2020-09-30T15:04:31.533Z",
    "updatedAt":"2020-09-30T15:04:31.533Z"
  },
  "securityAnswer":"a"
}
```

securitylab
CYBER SECURITY

Sec-lab.com

4 Febbraio 2021

Applicazioni

Nuovissimo Corso Web Application Hacking

Facundo Pantaleo: Senior Cyber Security Advisor Security Lab
Andrea Costantino:Senior Cyber Security Advisor Security Lab

Corso di Web Application Hacking

- Il nuovo corso di ''**Web Application Hacking**'' è pensato per gli studenti che hanno zero esperienza partendo dalle basi e introducendoli nel mondo della sicurezza delle applicazioni web.

- Il corso tratterà i principali problemi di sicurezza odierni da due punti di vista:
  - **attacco**: spiegazione delle vulnerabilità e come queste si possono sfruttare.
  - **difesa**: messa a fuoco su i principali punti da tenere in considerazione durante la fase di sviluppo di un'applicazione web.

- La teoria sarà integrata con esercizi e laboratori presenti sulla piattaforma implementata da Seclab dove è possibile eseguire attacchi e mettere in pratica una serie di tecniche di hacking.

- Il corso fornirà infine un esame finale con relativo attestato.

Corso di Web Application Hacking - Sommario

- Ripasso di HTML
- Architettura delle Applicazioni Web moderne
- Funzionamento base del protocollo HTTP
- Meccanismi di sicurezza più comuni
- Tipologie di attacco:
  - Autenticazione
  - Autorizzazione
  - Sessione
  - Logico
  - Back-end
  - Injection
- Laboratori e demo hands-on
- Analisi di frammenti di codice vulnerabile e relativa risoluzione

Corso di Web Application Hacking

SQLi. Classical or in-band.

*SELECT * FROM Users WHERE Username='$username' AND Password='$password'*

Suppose we insert the following Username and Password values:

$username = 1' or '1' = '1
$password = 1' or '1' = '1

Actual GET request:

http://www.example.com/index.php?username=1'%20or%20'1'%20=%20'1&password=1'%20or%20'1'%20=%20'1

The query will be:

*SELECT * FROM Users WHERE Username='**1' OR '1' = '1**' AND Password='**1' OR '1' = '1**'*

Corso di Web Application Hacking

XML External Entities

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<users>
<user id="111">
<username>seclab</username>
<password>123456 </password>
<email>course@sec-lab.com</email>
</user>
</users>
```

Root element

attribute

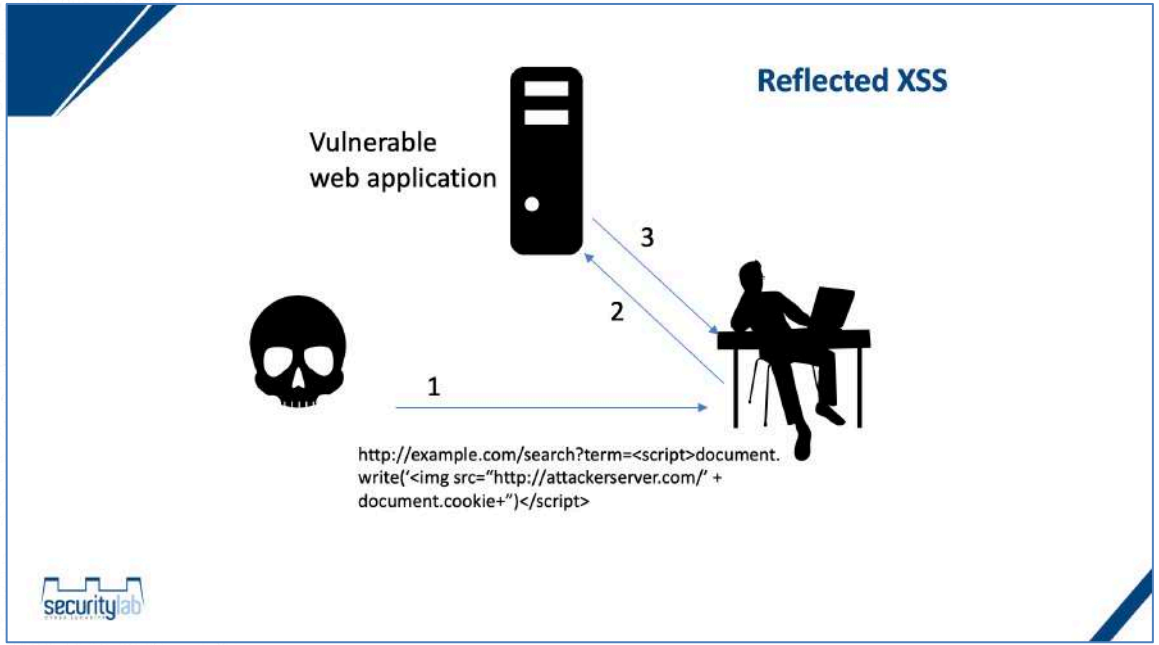
elements

In the example above can be seen several opening and corresponding closing tags, these are called **elements**.

There is only one **root element**, in particular in this example this is <users> </users>

There is another tag named user that has an associated **attribute** id having a value of 111. An attribute contains a value related to a tag.

Corso di Web Application Hacking



Corso di Web Application Hacking

XSS Faulty Code

No protections

```
<?php
    if($_GET['name'] == NULL || $_GET['name'] == ''){
        echo 'Hello ' . $_GET['name'];
}?>
```

Poorly implemented protection

```
<?php
    if($_GET['name'] == NULL || $_GET['name'] == ''){
        echo 'Hello ' . str_replace('<script>', '', $_GET['name']);
}?>
```

Recommended implementation

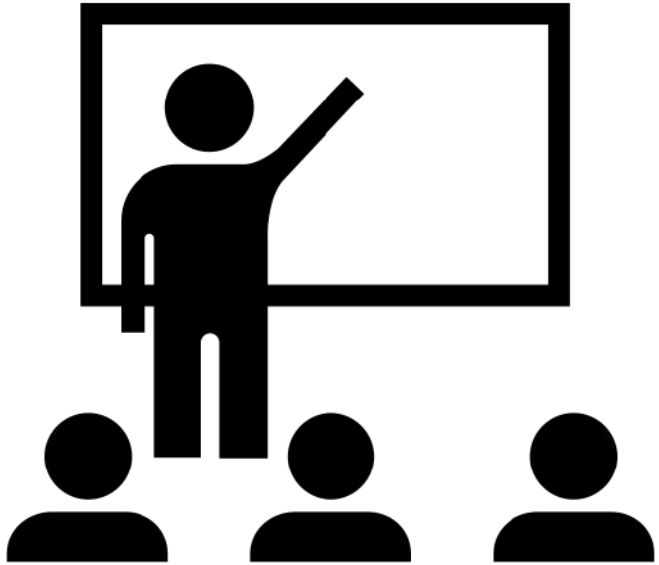
```
<?php
    if($_GET['name'] == NULL || $_GET['name'] == ''){
        echo 'Hello ' . htmlspecialchars($_GET['name']);
}?>
```

Corso di Web Application Hacking

Corso di Web Application Hacking

Corso di Web Application Hacking

- **Data da definirsi, primavera 2021**
- Maggiori informazioni sul sito www.sec-lab.com o iscrivendosi alla newsletter.
- ***sconto del 10% ai partecipanti di questo webinar e agli iscritti AITI***.



securitylab
CYBER SECURITY

Sec-lab.com

4 Febbraio 2021

L’anello debole della catena

Risorse umane

Sommario / Relatori

Andrea Costantino

Senior Cyber Security Advisor **Security Lab**

Come costruire una campagna di phishing per misurare la consapevolezza delle risorse umane

Alessandro Carniato

e-Learning Instructional Designer **Security Lab**

- L’esplosione della formazione e-Learning: opportunità e sfide
- E-Learning al servizio della Cyber Security: esempi di corsi interattivi

securitylab
CYBER SECURITY

Sec-lab.com

4 Febbraio 2021

Risorse umane

Come costruire una campagna di phishing per misurare la consapevolezza delle risorse umane

Andrea Costantino: Senior Cyber Security Advisor Security Lab

Misurare la vulnerabilità umana. Cosa significa?

Misurare la vulnerabilità umana significa mettere in campo le stesse tecniche utilizzate dai criminali informatici per far leva sulla scarsa consapevolezza, sui sentimenti, e sui desideri delle persone umane al fine di realizzare truffe o attaccare sistemi informatici.

- Phishing telefonico
- Disseminazione USB key
- Installazione dispositivi
- Campagna di Phishing

Campagna di Phishing
Preparazione di una campagna

- ☑ Definire gli obiettivi
- ☑ Definire lo scenario
- ☑ Definire i target
- ☑ Eseguire la pianificazione
- ☑ Preparare l’arsenale
- ☑ Lanciare la campagna
- ☑ Presentare i risultati

Campagna di Phishing
Definire gli obiettivi

- Gli obiettivi di una campagna possono attestarsi a diversi livelli di approfondimento. Alla base rimane sempre l'indurre la vittima ad eseguire operazioni o fornire informazioni che non dovrebbe.
- L'obiettivo può limitarsi alla verifica del grado di preparazione a fronte di comunicazioni (e-mail, telefonate, etc.) malevole.
- Quello principale rimane quasi sempre il furto di credenziali e/o informazioni personali.
- Ma può anche essere esteso all'esecuzione di comandi o applicativi sul dispositivo della vittima.

Campagna di Phishing
Definire lo scenario

- Una campagna di phishing per essere efficace deve essere coerente con il target alla quale è rivolta.
- Le vittime devono potenzialmente essere utenti effettivi del servizio che si vuole violare.

Campagna di Phishing
Definire i target

- Nel caso di uno scenario concordato i target vengono definiti con il cliente.
- In questo caso viene fornita una lista di nominativi e indirizzi da utilizzare per l'allestimento della campagna.
- Ulteriori informazioni (come dipartimento, posizione, etc.) possono aiutare a personalizzare la campagna e renderla di conseguenza più efficace.
- Nel caso di un attacco malevolo l'hacker deve procurarsi autonomamente tali informazioni, i metodi più comuni includono la violazione di servizi (web o altro), furto di dati, finti sondaggi, etc.

Campagna di Phishing
Eseguire la pianificazione

- **Creazione delle liste** di distribuzione e pianificazione temporale delle fasi di invio.
- **Registrazione di un dominio** con grafia simile all'originale (attacco omografico).
- **Oppure con grafia** riconducibile a possibili errori di digitazione (typosquatting).
- **Allestimento di un sito** clone il più simile possibile al sito web originale.
- **Preparazione della landing page** con funzionalità di cattura delle credenziali.
- **Allestimento di ulteriori landing pages** per il download di eseguibili malevoli.
- **Allestimento di un template** e-mail credibile.

Campagna di Phishing
Preparare l’arsenale

Tool utilizzati:

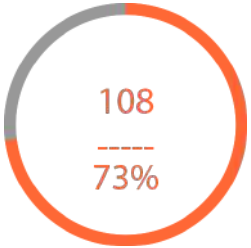
- **Phishing framework** per l'esecuzione della campagna.
- **Mail server** per l'intercettazione di eventuali messaggi di risposta.
- **Web server** per servire il clone del sito oggetto di phishing.
- **Exploitation framework** per l'esecuzione di attacchi rivolti al client. credibile.

Campagna di Phishing
Lanciare la campagna

- Invio delle email di phishing secondo la pianificazione temporale.
- Cattura delle credenziali e riutilizzo delle stesse (in caso di attacco reale).
- Exploiting del sistema in seguito all’esecuzione dell’applicazione malevole.

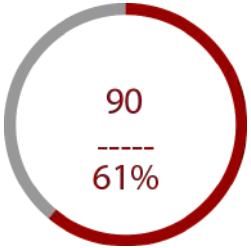
Campagna di Phishing

Caso reale

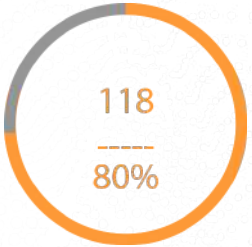


Clicked Link

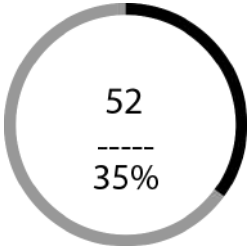
Email Sent



Submitted Data



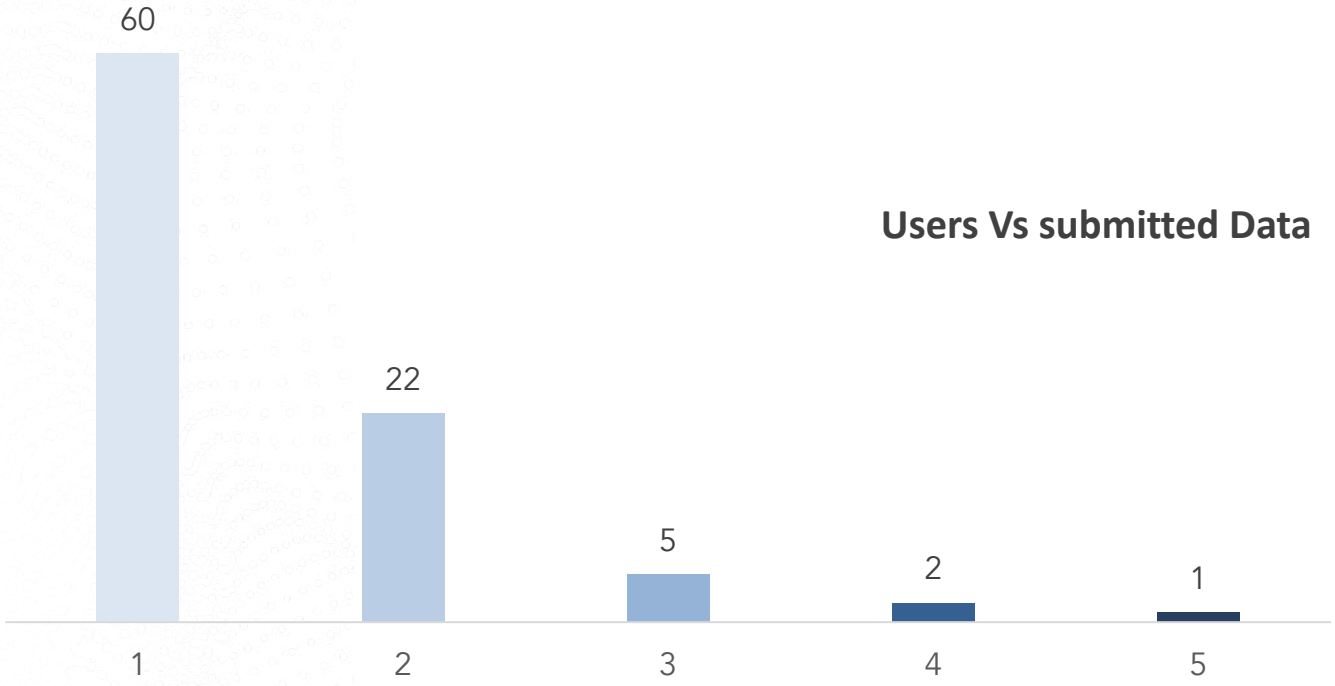
Email Opened



Ran Application

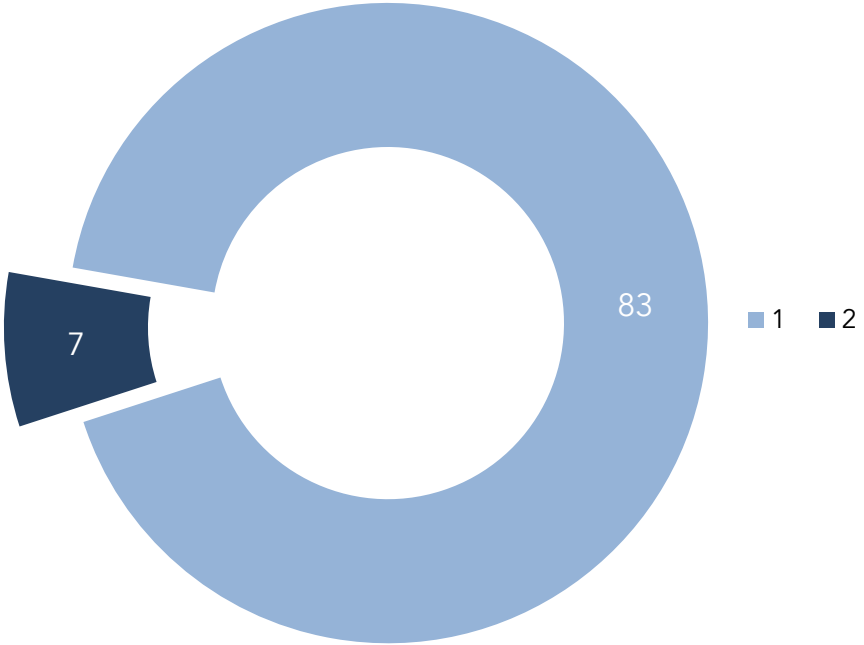
Campagna di Phishing

Caso reale -risultati



Campagna di Phishing

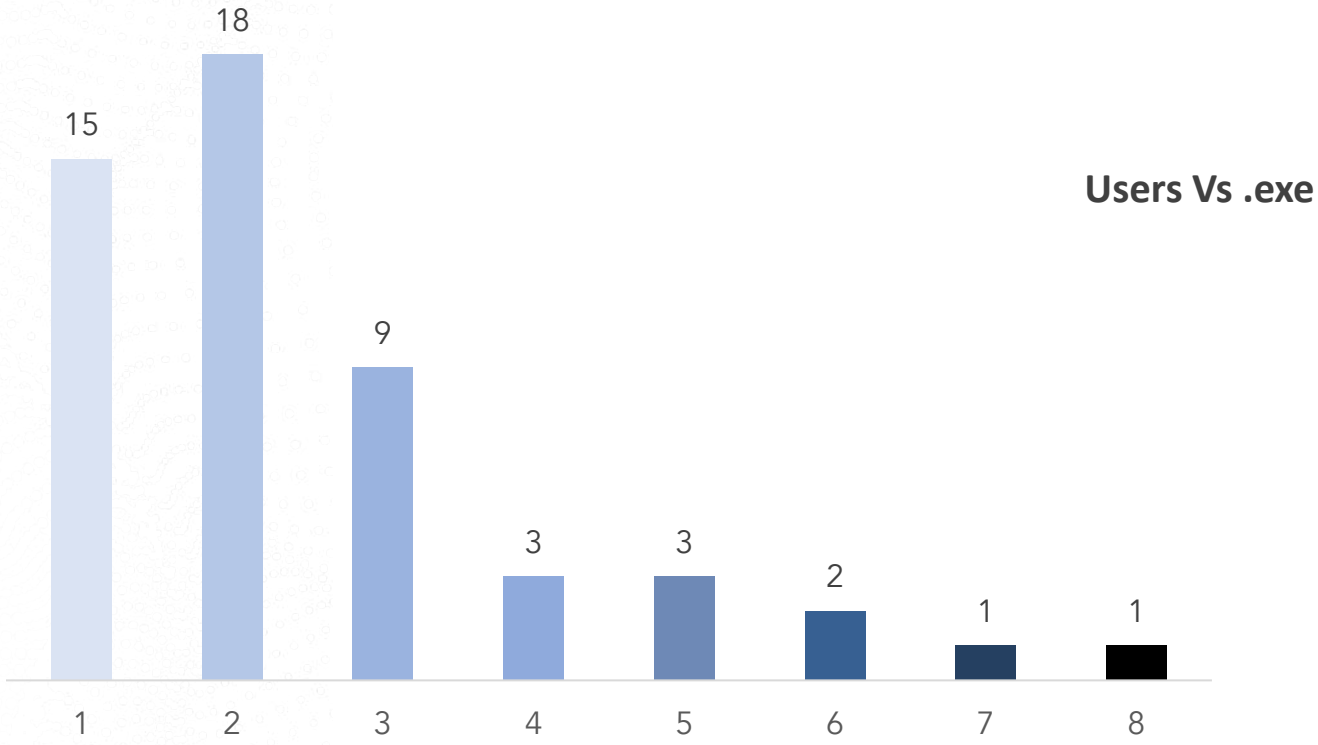
Caso reale -risultati



Users Vs different Data

Campagna di Phishing

Caso reale -risultati



Attacchi alla persona

Prevenzione

- Esecuzione di audit per la valutazione del livello di rischio.
- Formazione in azienda del personale a fronte delle minacce.
- Istruzione attraverso strumenti di formazione online (e-learning).

securitylab
CYBER SECURITY

Sec-lab.com

4 Febbraio 2021

Risorse umane

L’esplosione della formazione e-Learning: opportunità e sfide

Alessandro Carniato: e-Learning Instructional Designer Security Lab

securitylab
ACADEMY

E-learning al servizio della Cyber Security

- L’esplosione della formazione e-Learning: opportunità e sfide
- E-Learning al servizio della Cyber Security: esempi di corsi interattivi

Alessandro Carniato

E-learning project manager - Security Lab

Winston Churchill

Sono sempre pronto ad imparare; non sempre a lasciare che mi insegnino..

- Primo ministro del Regno Unito -

EFFICACIA

‘’Capacità di produrre pienamente l’effetto voluto, e l’ottenimento stesso dell’effetto..’’

’’Situazione di massima capacità produttiva, e cioè di costi minori possibili, in un complesso industriale, in un’attività commerciale, ecc..’’

EFFICIENZA

FACE TO FACE

Contatto diretto		Eccellente
Info meta-comunicative		Eccellente
Adattabilità argomenti		Discreta
Docente/motivazione		Eccellente
Concentrazione		Bassa
Dipendenza capacità docente		Alta

FACE TO FACE

Coinvolgimento attivo		Bassa
Personalizzazione		Bassa
Costi		Elevati
Aggiornamento		Bassa
Unidirezionalità		Alta
Fruibilità		Bassa

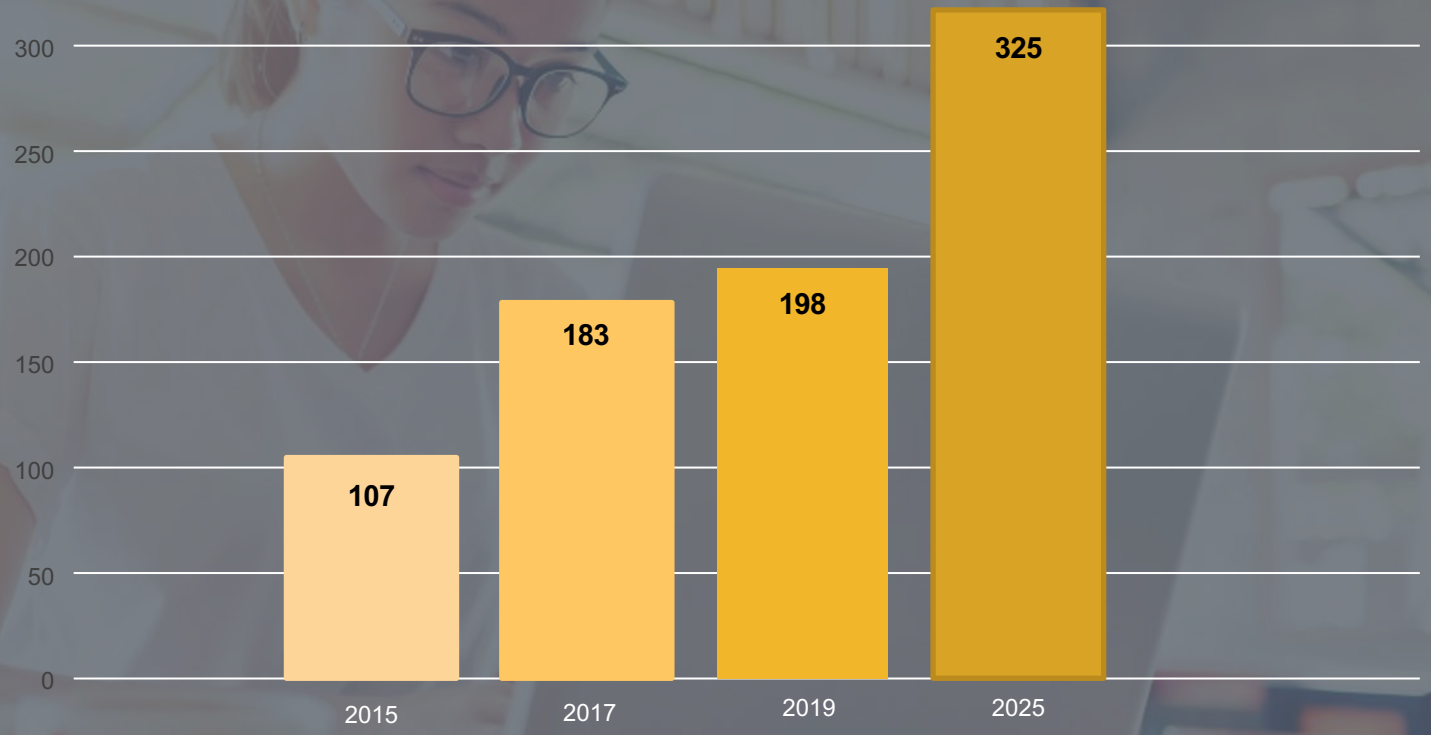
E-LEARNING

Lezioni multimediali interattive		Eccellente
Uniformare livelli conoscenza		Discreta
Standardizzazione insegnamento		Discreta
Aggiornamento rapido e tempestivo		Eccellente
Interazione diretta docente		Bassa
Assenza discenti		Bassa

E-LEARNING

Autogestione		Eccellente
Rivedere le lezioni		Eccellente
Condivisione dei contenuti didattici		Eccellente
Personalizzazione struttura		Discreto
Costi		Eccellente
Verifica e certificazione apprendimento		Molto buona

MERCATO GLOBALE E-LEARNING (BILLION)



Fonte: Global Market Insights; eLogic Learning

77%

Organizzazioni formano online

Fonte: Ambient Insight

40-60%

Risparmio di tempo dipendenti

Fonte: Brandon Hall Study

25-60%

Retention rate

Fonte: Brandon Hall Study

218%

Aumento entrate/dipendente

Fonte: Deilotte

Mercato mobile learning

67%

Organizzazioni

99%

Soddisfazione degli utenti

$37,6 Billion 2020

Fonte: Worldwide self-paced e-learning market revenue from 2016 to 2021

Importanza della formazione

1.500$/dipendente = +24%

Le aziende che investono sulla formazione dei dipendenti registrano un incremento significativo dei profitti

Fonte: America Society for Training and Development (2500 aziende)

IBM: + 200 million $

Importanza della formazione

1$/e-learning = 30$ produttività

IBM ha dimostrato che i guadagni di produttività derivano dalla capacità dei dipendenti di applicare immediatamente le loro nuove competenze acquisite

Fonte: IBM

Velocità di apprendimento

Velocità di apprendimento/h: 5X

IBM ha scoperto che gli iscritti ai corsi di e-learning hanno imparato cinque volte più velocemente rispetto alle lezioni tradizionali, consentendo all'azienda di realizzare significativi risparmi sui costi

Fonte: IBM

Risparmio economico

50% - 70%

Le aziende risparmiano dal 50% al 70% quando sostituiscono la formazione *face to face* con l'e-learning

Fonte: Intitute of Management ad Amministration Survey

IBM: + 200 million $

Formazione

75%

dei leaders accedemici include l’e-learning nei propri programmi didattici

96%

delle università degli Stati Uniti offre dei corsi in modalità e-learning

Fonte: Babson Survey Research Group

233,000,000+

Utenti in tutto il mondo

30,000,000+

Corsi erogati

159,000+

Siti attivi

239

Paesi in cui è utilizzato

securitylab
CYBER SECURITY

Sec-lab.com

4 Febbraio 2021

Risorse umane

e-Learning al servizio della Cyber Security: esempi di corsi interattivi

Alessandro Carniato: e-Learning Instructional Designer Security Lab

Vantaggi per gli iscritti

Per tutti gli iscritti verranno riconosciuti i seguenti vantaggi:

- **Incontri di approfondimento one-to-one** senza impegno per le varie tematiche, 9 e 10 febbraio dalle 14:00 in poi con prenotazione tramite AITI servizi
- **Possibilità di organizzare un POV (Proof of Value)** di un mese della tecnologia Darktrace in azienda, senza alcun impegno, con il supporto diretto di Security Lab e Darktrace
- **Sconto 20%** sulle soluzioni e-Learning dell'e-Learning Atelier con la possibilità di richiedere una demo interattiva in modalità SaaS del corso di Security Awareness
- **Sconto 10%** sul nuovo corso Web Application Hacking che verrà pianificato a breve

securitylab
CYBER SECURITY

Sec-lab.com

4 Febbraio 2021

Grazie per l’attenzione

Domande?