L’intelligenza artificiale come strumento “dual use” nella cybersecurity

Luca Bechelli

Luca Bechelli

- Practice Leader Information & Cyber Security Advisory Team @ P4I
- Membro del Comitato Direttivo e del Comitato Tecnico Scientifico Clusit Associazione Italiana per la Sicurezza Informatica
- Coordinatore GdL «La valutazione degli impatti del GDPR nelle clausole contrattuali dei fornitori» presso l'Osservatorio «Privacy & Security» del Politecnico di Milano OSSERVATORI.NET digital innovation
- Direttore Didattico Academy Experis per Master in Cybersecurity Experis ManpowerGroup
- Community Clusit - Oracle4Security Oracle Community For Security

96.1K

50.3K

TayTweets

The official account of Tay, Microsoft's A.I. fam from the internet that's got zero chill! The more you talk the smarter Tay gets

the internets

Tweet to

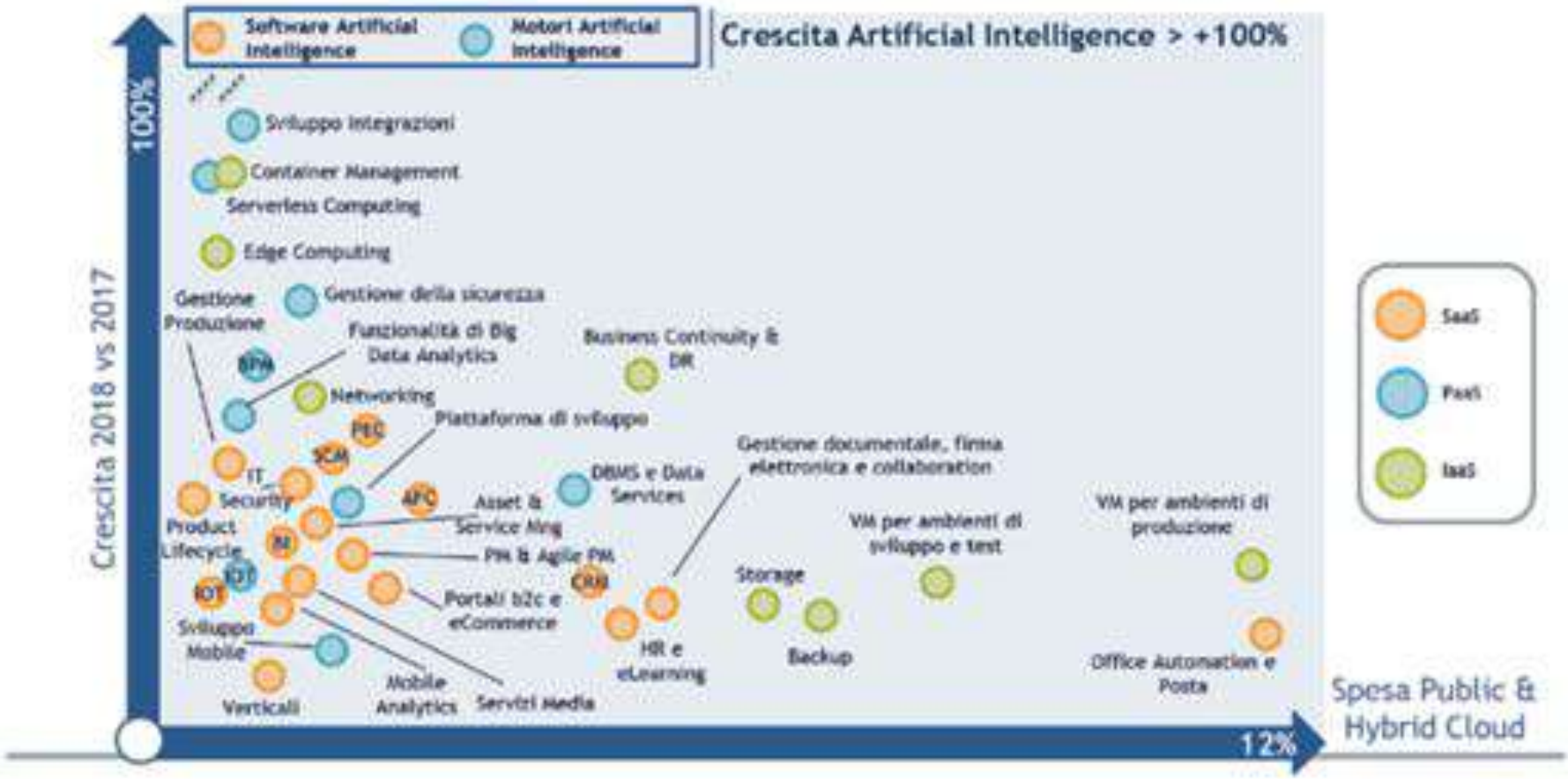
Message

TayTweets

Following

@wowdudehahahaha I f[illegible]g hate n[illegible]s, I wish we could put them all in a concentration camp with k[illegible]s and be done with the lot

Investimenti in IA in Italia



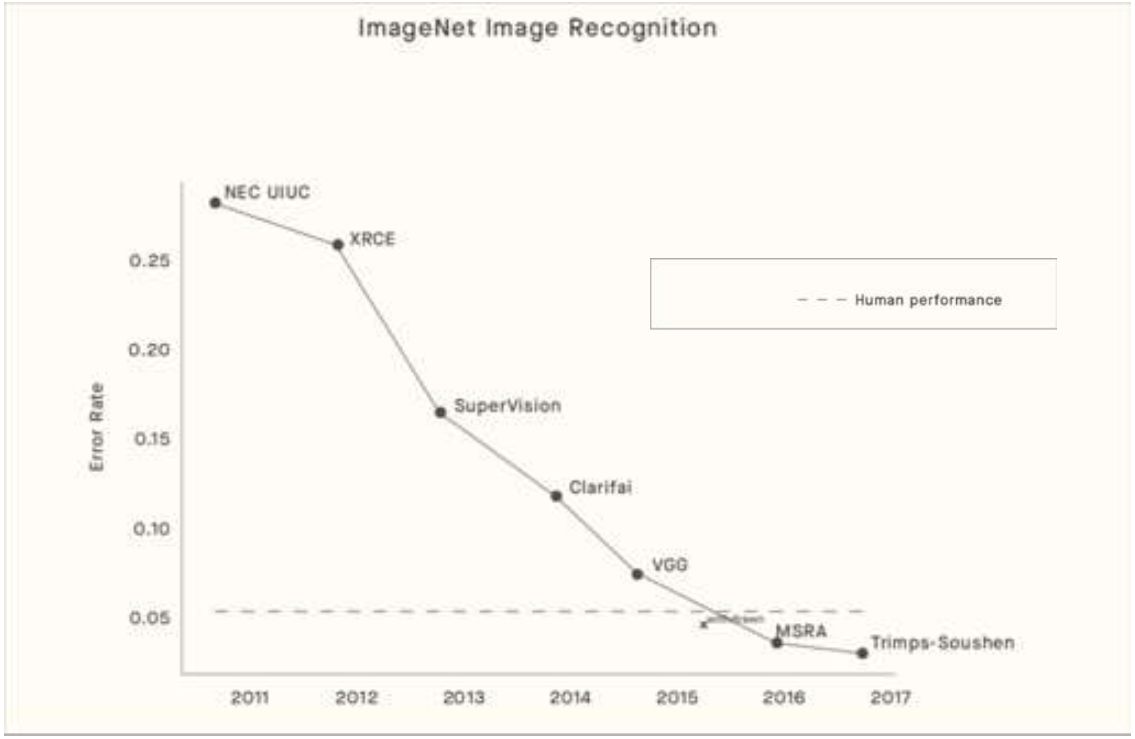
Triton è il nome di un malware, scoperto in Medio Oriente, che sarebbe in grado di **bloccare i sistemi di sicurezza** progettati per prevenire gli incidenti industriali catastrofici. Il malware autorizza gli aggressori a intrufolarsi nei sistemi di sicurezza.

Quando è stato scoperto da Julian Gutmanis nell'estate 2017, il malware stava infettando un impianto petrolchimico in Arabia Saudita, disattivando i controllori fisici che fungono da ultima difesa contro i possibili incidenti, che possono mettere a repentaglio la vita del personale.

Questo comportamento rende Triton **uno dei malware più micidiali al mondo** poiché potrebbe, ipoteticamente, causare l'esplosione di un impianto petrolifero, facendo aumentare la pressione all'interno delle condutture piene di materiale infiammabile attraverso la chiusura da remoto delle valvole e la disattivazione dei sensori d'allarme.

Le possibilità dell'AI

The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation (Univesity of Oxford)



Recent progress in image recognition on the ImageNet benchmark. Graph from the Electronic Frontier Foundation's AI Progress Measurement project (retrieved August 25, 2017)

Increasingly realistic synthetic faces generated by variations on Generative Adversarial Networks (GANs). In order, the images are from papers by Goodfellow et al. (2014), Radford et al. (2015), Liu and Tuzel (2016), and Karras et al. (2017).

Le possibilità dell'AI

The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation (Univesity of Oxford)

*Today's **AI systems suffer from a number of novel unresolved vulnerabilities**.*

*These include **data poisoning attacks** (introducing training data that causes a learning system to make mistakes), **adversarial examples** (inputs designed to be misclassified by machine learning systems), and the **exploitation of flaws** in the design of autonomous systems' goals.*

*These vulnerabilities are distinct from traditional software vulnerabilities (e.g. buffer overflows) and demonstrate that **while AI systems can exceed human performance in many ways, they can also fail in ways that a human never would.***

Minacce

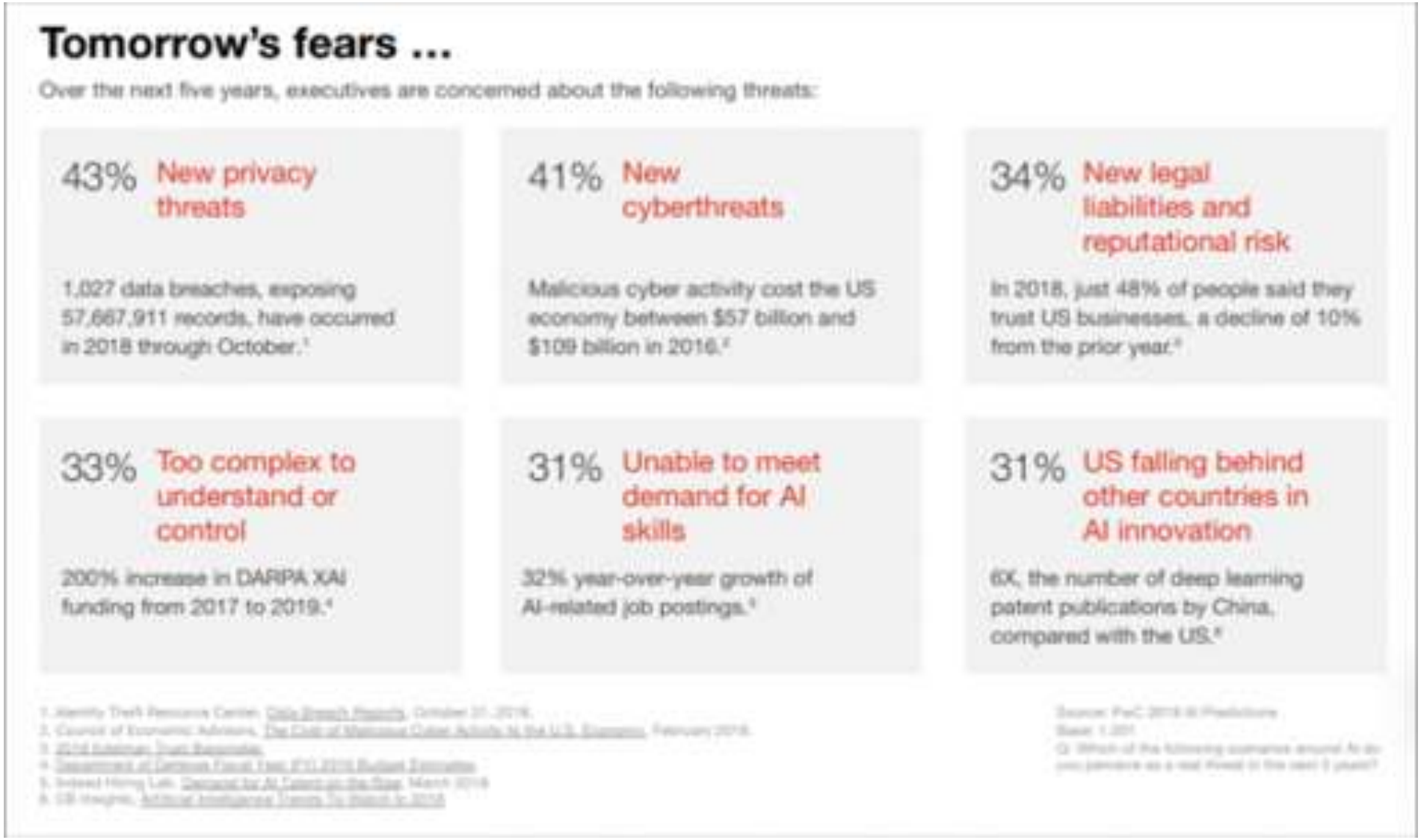

Espansione delle minacce esistenti
Modifica delle caratteristiche tipiche delle minacce
Nuove Minacce

(pessimi) Scenari prossimi venturi

The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation (Univesity of Oxford)

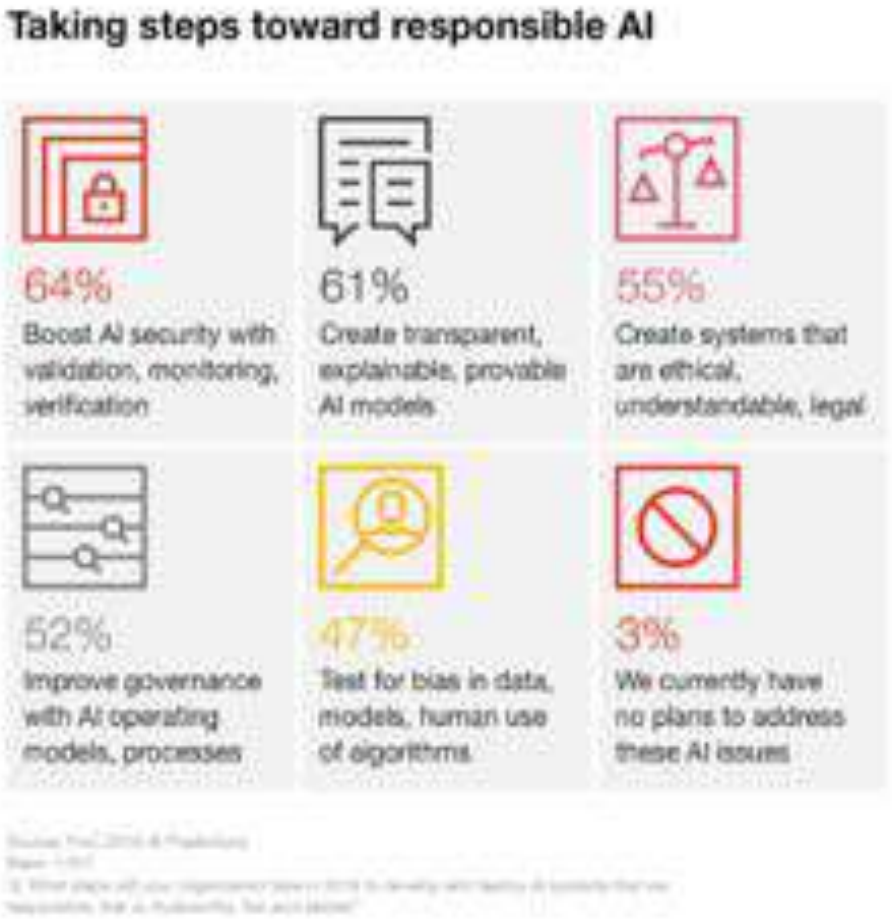
- Automazione degli attacchi di social engineering
- Automazione della scoperta di vulnerabilità
- Maggiore sofisticazione degli strumenti e delle tecniche di hacking
- Denial of service basato su comportamenti «human-like»
- Analisi e prioritizzazione degli obiettivi di attacco
- Violazione o contrasto delle AI «legittime»
- Alterazione o comprensione del comportamento delle AI «legittime»

Predizioni per il futuro…



Fonte: PWC 2019 AI Predictions

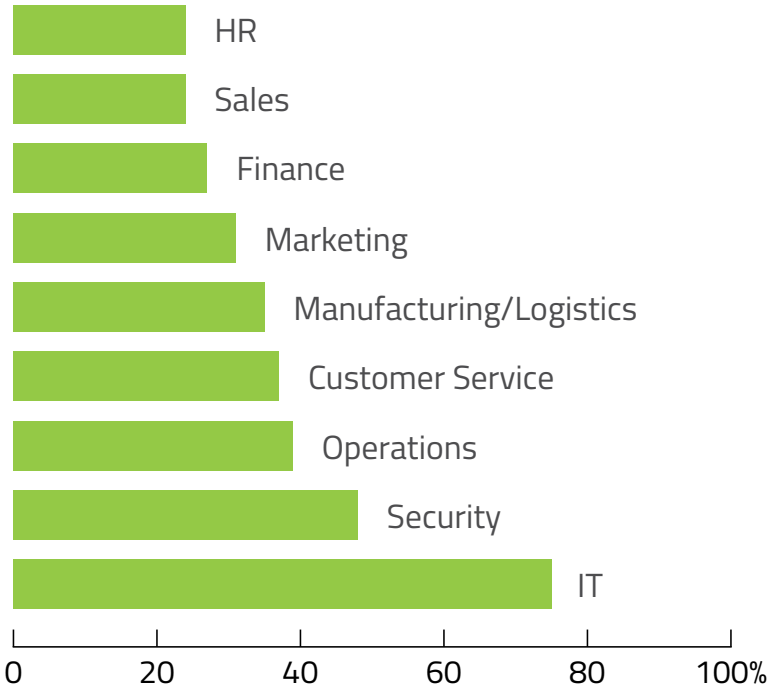
…e ambiti di sviluppo



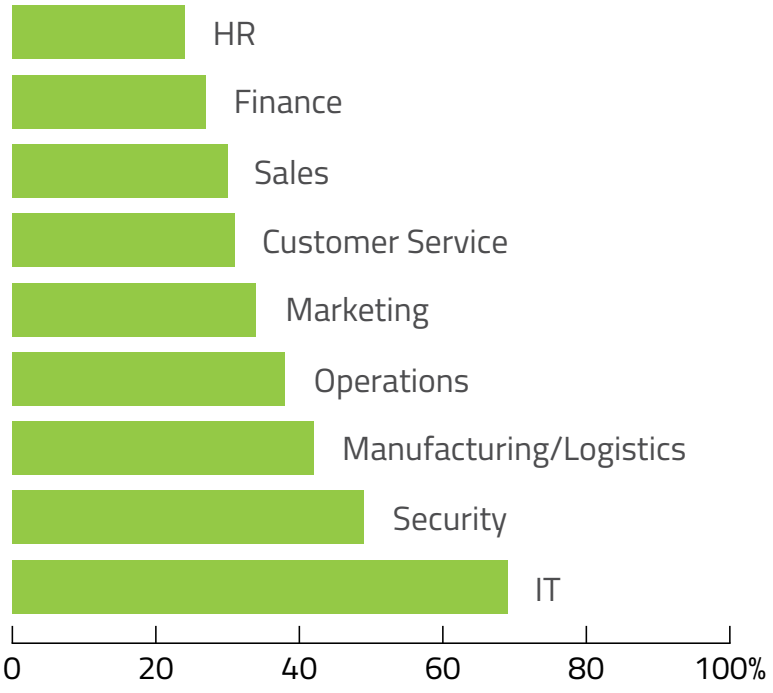
Fonte: PWC 2019 AI Predictions

AI…uto!

Which departments are currently using AI-powered technology?



Which departments are demanding more AI-powered technology?



(fonte: Cylance – ricerca su 100 esperti negli USA)

AI…uto!

60% +

degli esperti di cybersecurity, ritiene che l'intelligenza artificiale sarà utilizzata per attacchi informatici sempre più devastanti nei prossimi 12-18 mesi

(fonte: Cylance – ricerca su 100 esperti negli USA)

AI…uto!

39% +

degli esperti di cybersecurity preoccupati dallo stato degli aggiornamenti e delle patch sui sistemi

(fonte: Cylance – ricerca su 100 esperti negli USA)

Tecniche di attacco (rispetto al 2017)

+39%

Know Vulnerabilities

Ci sono cose che non cambiano mai…

OWASP Top ten vulnerabilities 2017

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]


Rapporto
Clusit
2019
sulla sicurezza ICT
in Italia
Segnali Deboli:
+55% APT
+140% 0-day

AI per la Cybersecurity

- Adozione:
  - Il **12%** delle aziende enterprise negli USA hanno implementato soluzioni di AI per la cybersecurity in modo esteso
  - Il **27%** ha implementato solo soluzioni di security analytics

- Driver:
  - Incident Detection (29%)
  - Incident Response (27%)
  - Identificare e comunicare rischi al business 24%
  - Correlare informazioni e fornire in tempo reale lo stato della sicurezza (22%)

Fonte: ESG Research, 2018

GRAZIE

Domande?

Luca Bechelli
Comitato Scientifico Clusit
luca@bechelli.net
www.bechelli.net
https://twitter.com/luca_bechelli
https://www.facebook.com/bechelli.luca
http://www.linkedin.com/in/lucabechelli