Cybersecurity e Just Culture: dall’errore alla resilienza aziendale

Giorgio di Grazia | Pre-Sales Specialist, *Deda Tech*

Giorgio di Grazia
Pre-Sales Specialist, Deda Tech

30	Anni di esperienza in ambito IT, 20 di IT Security
10	Anni di esperienza come pentester
7	Anni di assessment PCI DSS (PCI QSA, PA-QSA)
6	Anni come Technical Product Manager (Threat Detection and Response) e Pre-Sales (MDR)

Just Culture

Just Culture

Just Culture 1/2

”

Just Culture [is] as an *atmosphere of trust* in which people are encouraged, and even rewarded, for providing essential *safety-related* information, but in which they are also clear about where the line must be drawn between *acceptable* and *unacceptable behaviour*.

James Reason, British professor of psychology at the University of Manchester

Photo by Pixabay

Just Culture 2/2

”

A just culture means getting to an account of *failure* that can do two things at the same time: satisfy demands for *accountability*; contribute to *learning* and *improvement*. Accountability that is backward-looking tries to find a *scapegoat*. But accountability is about *looking ahead*.

Sidney Dekker, University of Brisbane, “Just Culture. Balancing Safety and Accountability”

Photo by Pixabay

Blame culture: l’opposto della just culture

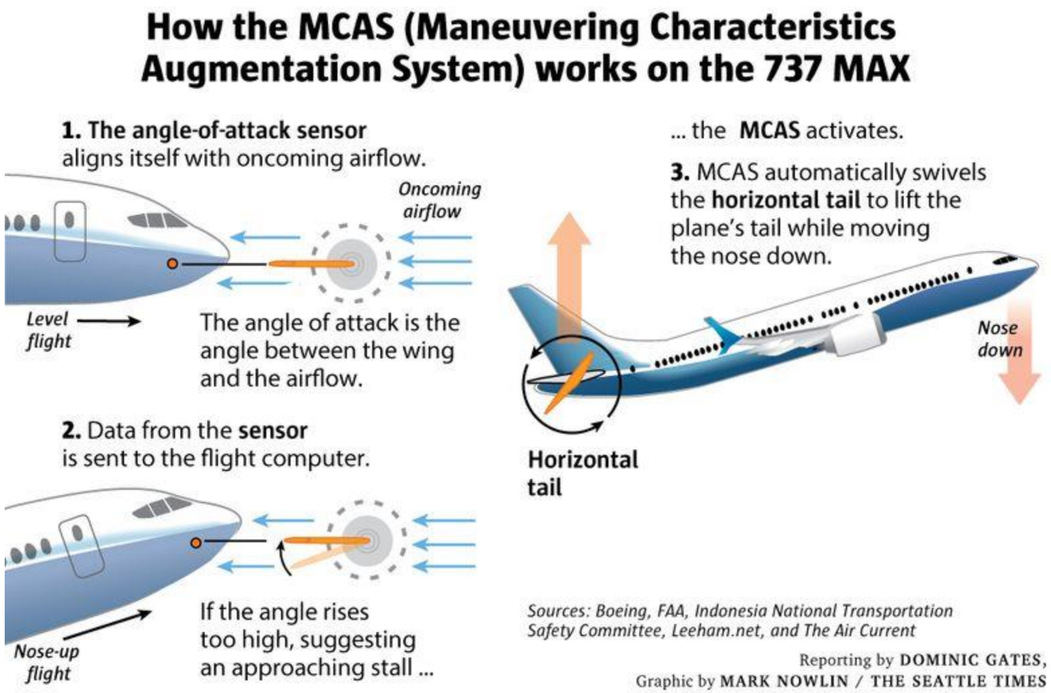
- La **blame culture** è un ambiente in cui le persone vengono spesso individuate, criticate e incolpate per gli errori e le mancanze.
- Le persone sono riluttanti ad assumersi la **responsabilità** delle proprie azioni e dei propri errori, poiché temono le critiche e i **rimproveri** dei manager.
- Risultato? Un ambiente **statico** che non permette di ridurre gli **errori umani**.

Just Culture: aviazione e sanità

- Nell'industria dell'**aviazione** (ma anche della **sanità**), i dipendenti sono incoraggiati a segnalare incidenti ed errori senza timore di punizioni.
- Le persone devono però agire in **buona fede** e non **violare** intenzionalmente regole o procedure.
- Questo permette di scoprire cosa è andato storto e di sviluppare nuovi processi o **formazione** per evitare che incidenti simili si ripetano in futuro.

Il volo Lion Air 610 (Boeing 737 MAX 8)

Il volo Lion Air 610: l'incidente



- 29 ottobre 2018: il volo **Lion Air 610** si schianta dopo il decollo da Giacarta uccidendo tutti i 189 passeggeri a bordo: il primo incidente mortale di un Boeing 737 MAX.
- Il nuovo **Boeing 737 MAX 8** prevede motori più grandi rispetto ai vecchi 737. Problema: rischio di destabilizzazione del beccheggio.
- Boeing decide quindi d'installare un software anti-stallo, il *Maneuvering Characteristics Augmentation System* (**MCAS**).
- Il MCAS si attiva con un sensore **AoA** (*Angle of Attack*).
- Il malfunzionamento di questo sensore causa l'incidente (e anche il successivo sul volo **Ethiopian Airlines 302**).

Cosa è accaduto in sintesi

1.	I dati del sensore AoA erano errati, probabilmente a causa di una **calibrazione** non corretta (non rilevata).	GUASTO
2.	I problemi presenti nel volo precedente non sono stati **documentati** correttamente.	ERRORE UMANO
3.	Boeing ha progettato MCAS per basarsi sui dati provenienti da un singolo sensore (**single point of failure**).	ERRORE PROGETTAZIONE
4.	La Boeing non ha classificato il sensore come un sistema critico, sottovalutando i **rischi** associati.	ERRORE PROCEDURA
5.	Boeing presupponeva che i **piloti** potessero rispondere rapidamente a qualsiasi malfunzionamento.	ERRORE PROCEDURA
6.	I piloti non sono stati adeguatamente **formati** su come riconoscere e rispondere all'attivazione del MCAS. I piloti non hanno **reagito** correttamente.	ERR. PROC./UMANO
7.	Boeing ha scelto di non enfatizzare l'MCAS nella **formazione** per evitare costose sessioni basate su simulatori.	COMPLIANCE
8.	Il processo di **certificazione** della Boeing è diventato sempre più autoregolamentato.	COMPLIANCE

Il volo Lion Air 610: Error Traps

> No single individual acted outside their envelope of normal performance variation, let alone recklessly. It was an accident waiting to happen.
>
> Elmar Lutter, President & CEO at Lufthansa Technik Philippines, “Error Traps”

Photo by Pixabay

Dekker: human error investigation

”

Remember that the point of a human error investigation is to understand why people did what they did, not to judge them for what they did not do.

Sidney Dekker, “The Field Guide to Human Error Investigations”

Photo by Pixabay

Just culture e cybersecurity

Possiamo applicare questo approccio al nostro mondo cyber?

Possibili risposte agli errori umani

ERRORE → COLPA

Errore involontario	Comportamento a rischio	Comportamento a rischio reiterato	Comportamento incurante del rischio
Comportamento non intenzionale.	Comportamento intenzionale, rischio sottostimato.	Violazione deliberata e ripetuta di policy e procedure.	Rischio non giustificabile, comportamento consapevole.
Risposta: azione correttiva, l'errore può essere giustificato.	**Risposta**: azione correttiva, formazione del dipendente/gruppo.	**Risposta**: azione correttiva e punitiva.	**Risposta**: azione punitiva.

Altri errori

Altri errori non legati al singolo individuo: sistemi, procedure, cultura e gerarchia.

I protagonisti del nostro caso cyber

Marco, *sysadmin*

Società industriale italiana

Luca, *analista SOC*

Società industriale italiana

Paolo, *grande bevitore*

Amico di Marco, non lavora

Generated with ThisPersonDoesNotExist.com (StyleGAN2, an advanced generative adversarial network)

Il caso cyber: l’incidente

- È venerdì sera. **Marco** (IT) è rimasto solo in ufficio e ha il compito di modificare le regole del **firewall** per limitare l’esposizione di un sistema di **produzione**.
- In mattinata, **Luca** (SOC) ha segnalato al reparto IT la necessità di limitare il traffico per mitigare uno **0-day**.
- **Marco** ritiene che non vi sia urgenza, non modifica le regole del firewall ed esce prima per incontrarsi con l’amico **Paolo**.
- Poche ore dopo, un **attaccante** identifica in modo casuale la vulnerabilità e la sfrutta con un **exploit**.
- L’intera **DMZ** è compromessa in pochi minuti.

Il caso cyber: Marco è ritenuto l'unico responsabile

ERRORE → COLPA

Comportamento a rischio

Comportamento intenzionale, rischio sottostimato.

Risposta: azione correttiva, formazione del dipendente/gruppo.

Marco ha agito basandosi sull'esperienza pregressa (*bias*).

Non è compito di Marco fare una valutazione del rischio (*accettazione*).

I problemi complessi

”

For every complex problem, there is an answer that is clear, simple and wrong.

H. L. Mencken, American journalist, essayist, satirist, cultural critic

Photo by Pixabay

Il caso cyber: un’analisi più approfondita 1/3

1. Mancanza di una cultura della sicurezza

- Se Marco ha deciso di non intervenire subito è perché nell’azienda non c’è una vera **cultura della sicurezza**.
- Le segnalazioni del SOC vengano percepite come **allarmismi** e ignorate senza conseguenze.

ERRORE PROCEDURA

COMPLIANCE

ERRORE CULTURALE

2. Assenza di una procedura d’emergenza chiara

- Se ci fosse stata una **procedura formale** con un livello di escalation ben definito, Marco avrebbe agito diversamente.
- Manca un sistema di **tracciamento** delle segnalazioni con obbligo di presa in carico e conferma della **mitigazione**.

ERRORE PROCEDURA

COMPLIANCE

Il caso cyber: un’analisi più approfondita 2/3

3. Comunicazione inadeguata tra SOC e IT

ERRORE PROCEDURA

COMPLIANCE

- Il SOC non ha fornito dati sufficienti per far capire la **gravità** della situazione.
- Se la comunicazione non è chiara il rischio viene **sottovalutato**.

4. Carico di lavoro e risorse insufficienti

STAFF INSUFFICIENTE

COMPLIANCE

- Marco era da solo. L’azienda non ha un team di reperibilità per gestire **emergenze** di sicurezza.
- Il team IT è **sovraccarico** di lavoro. Il sistemista ha sottovalutato il problema perché stanco e demotivato.

Il caso cyber: un’analisi più approfondita 3/3

5. Problemi nella segmentazione della rete

ERRORE PROGETTAZIONE

COMPLIANCE

- Il fatto che l’intera **DMZ** sia stata compromessa indica che la rete non era strutturata per contenere un attacco.
- Le numerose **segnalazioni** di Marco al responsabile IT in merito alla necessità di rivedere la segmentazione sono state ignorate.

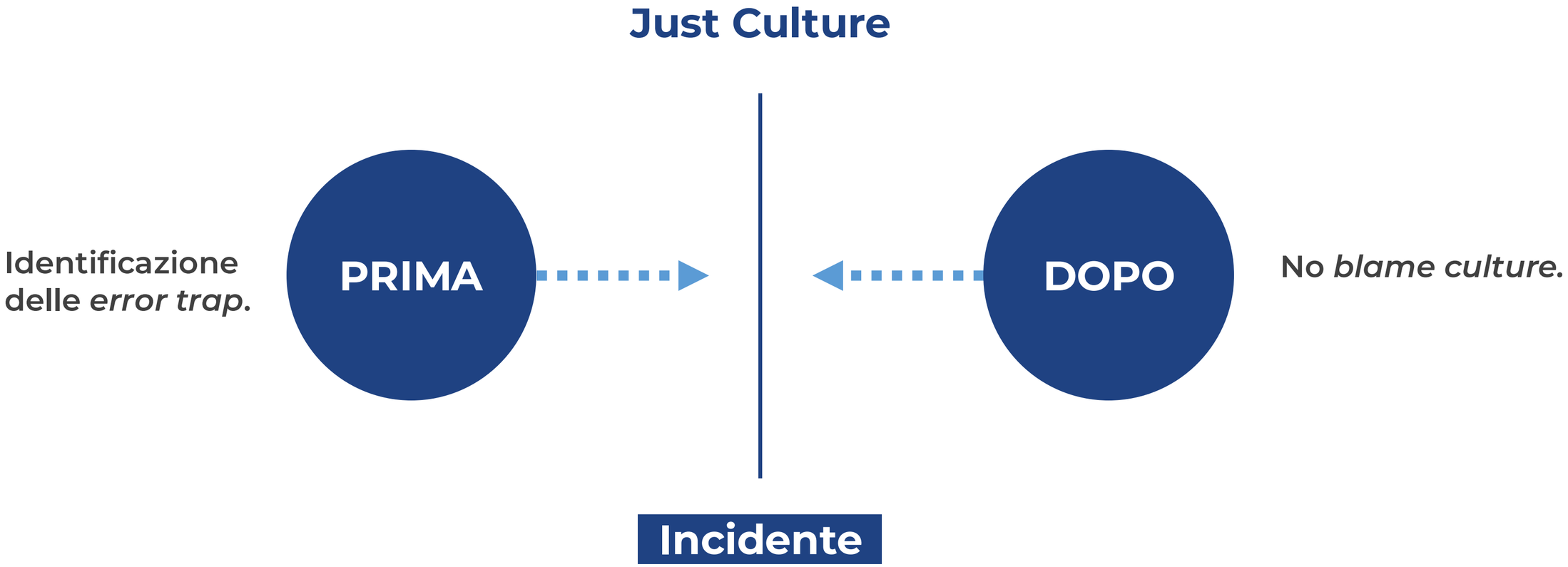
6. Errori tecnici e di gestione del rischio

ERRORE UMANO

ERRORE PROGETTAZIONE

- La mancata applicazione delle regole firewall ha lasciato aperta la porta all’attacco.
- Se il cambio delle regole del firewall fosse stato **automatizzato** il fattore umano avrebbe inciso meno.

Just Culture: prevenire e curare



A safety culture

”

A safety culture is a culture that allows the boss to hear bad news.

Sidney Dekker, “The Field Guide to Human Error Investigations”

Photo by Pixabay

Errori e problemi 1/2

Principio #1 – Gli errori e i problemi sono inevitabili. A volte generano incidenti.

Errori e problemi 2/2

Corollario #1 – La domanda è "Cosa è andato storto?" e non "Chi ha causato il problema?".

Just Culture e Cybersecurity

Ridurre i margini d’errore

Il giusto insieme di strumenti, tecnologie e procedure restringe il margine di errore degli esseri umani.

Scrivere policy utili

Se nessuno osserva una policy, valutare attentamente perché. Scrivere policy per difendersi dagli attacchi reali.

Motivare le persone

Anche chi commette *meno* errori riceve suggerimenti su come migliorare il proprio comportamento.

Segnalazioni formali

Stabilire meccanismi formali di segnalazione (anche *anonimi*) e indagine sugli incidenti (senza pregiudizi).

Training e awareness

Utilizzare gli incidenti come opportunità di apprendimento per migliorare le procedure.

Non sostituirsi a HR

La *Just Culture* non sostituisce gli uffici legale/HR e va utilizzata insieme alle politiche organizzative.

La cultura della sicurezza è di tutti 1/2

- Creare una cultura della **condivisione dei rischi** (Dino Dai Zovi, Black Hat 2019).
- Il team di security non deve rimanere **isolato**, ma interagire con gli altri team aziendali.
- Un esempio? Gli sviluppatori che scrivono funzioni di sicurezza devono poter chiedere una valutazione al team di security.
- Ciò comporta l'implementazione di un processo *post-mortem* **privo di colpe** quando si tratta di valutare un report delle vulnerabilità o un'anomalia.
- La sicurezza è un problema di **tutti**.

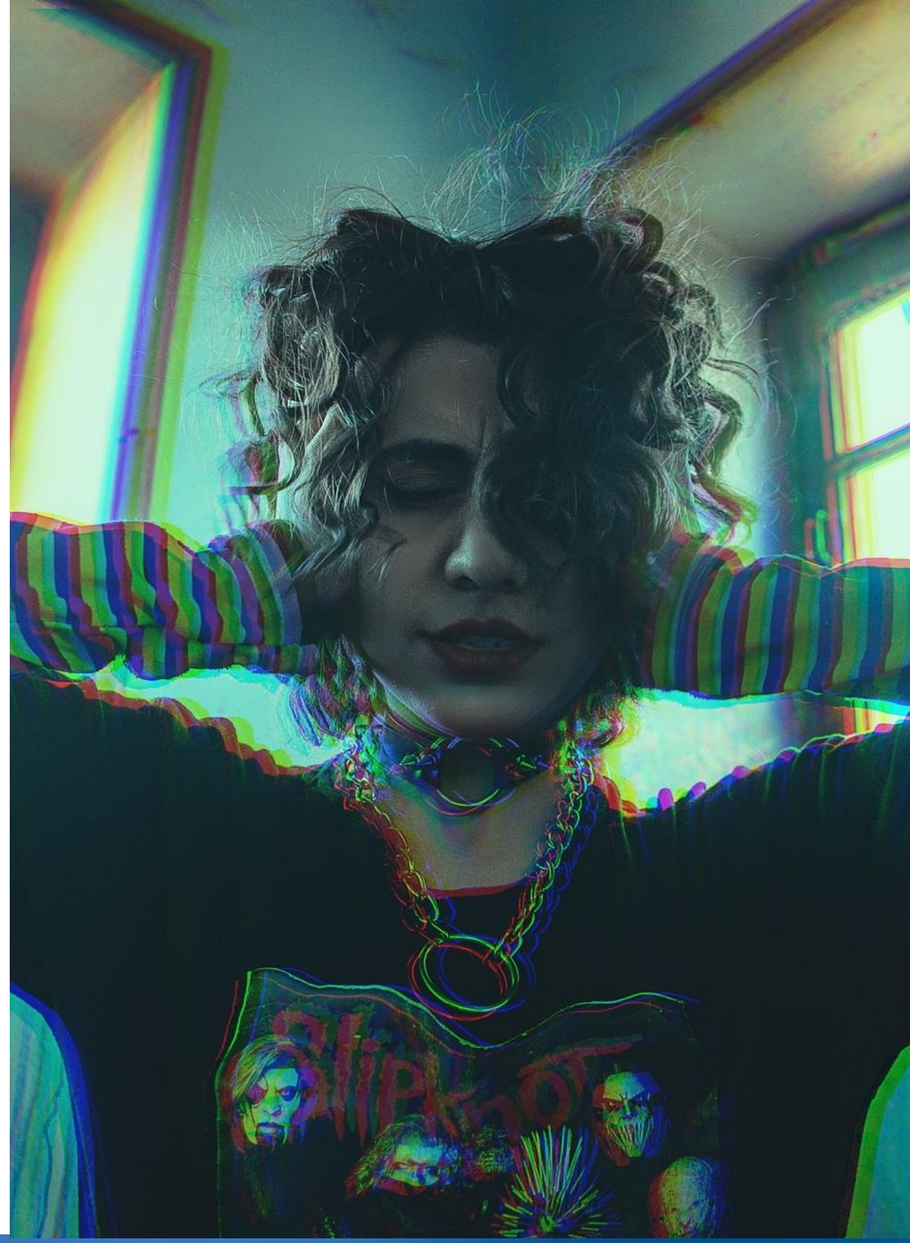


Photo by Elyas Pasban on Unsplash

La cultura della sicurezza è di tutti 2/2

”

Culture is way more powerful than strategy, which is way more powerful than tactics.

Dino Dai Zovi, hacker, infosec veteran, entrepreneur, “Black Hat 2019”

Photo by Pixabay

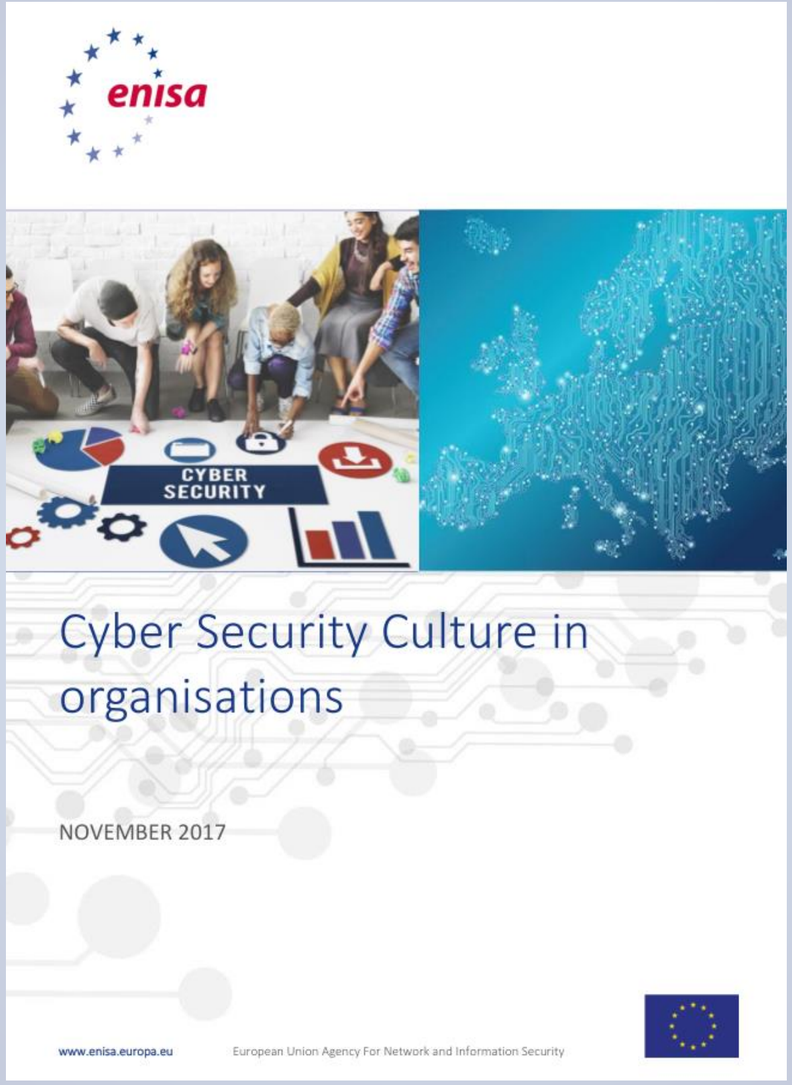
ENISA

Cyber Security Culture in organisations (2017)

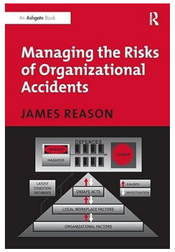
Il report attinge da più discipline, tra cui scienze organizzative, psicologia, diritto e sicurezza informatica.

- Definizione del concetto di Cyber Security Culture (CSC)
- Suggerimenti per l'implementazione del programma
- Elementi per costruire i programmi CSC
- Come misurare i programmi ecc.

"Humans possess a finite capacity for complying with security requests within the workplace. Beyond a certain threshold, any attempts to impose additional security procedures and requirements will be met by resistance and attempts to circumvent." (par. 8.4)

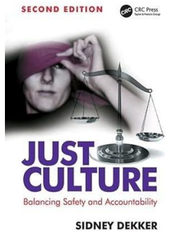


Approfondimenti indispensabili



Managing the Risks of Organizational Accidents

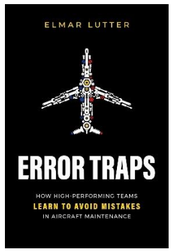
Di **James Reason** – 28 dicembre 1997



Just Culture: Balancing Safety and Accountability

Di **Sidney Dekker** – 22 giugno 2012

Just Culture (The Movie): https://sidneydekker.com/films/



Error Traps: How High-performing Teams Learn to Avoid Mistakes in Aircraft Maintenance

Di **Elmar Lutter** – 1° febbraio 2024

Incident management: come lavoriamo in **Deda Tech**

L’offerta Deda Tech

deda.tech

WHERE

On Premise
Le macchine del cliente, presso il cliente

@Hyper
Il cloud degli hyperscaler, gestito da noi

@Home
Un pezzo del nostro cloud, presso il cliente

@Deda
Il nostro cloud italiano libero

WHAT

MULTICLOUD BY DESIGN

Multicloud & Infrastructure
- Clouding @Deda
- Clouding @Home
- Clouding @Hyper
- Connecting Networks On Premise

Managed Services
- ManS for IT
- ManS for Hyper
- ManS for Security
- ManS for Enterprise AP

SOLUZIONI
- Managed IaaS
- Managed SAP
- Managed Stealth

SERVIZI SECURITY

Assessing
- Vulnerability Management
- Penetration Test & Red Team Services
- Network Security Assessment
- CISO Office as a Service

Advising
- Risk Assessment
- Business Impact Analysis
- Security Awareness

Protecting
- Cloud Security Services
- Network Security
- Vaulting & Recovery

Guarding
- Managed Detection & Response via SOC
- Red Button
- Threat Intelligence

HOW

Project, 10x5 or 24x7
Sviluppiamo progetti e prendiamo in gestione quello che ti serve, quando ti serve

Customer Success Manager
I tuoi partner ogni giorno al tuo fianco per trarre il massimo dai nostri servizi

User Centric SLAs
Misuriamo il successo dei nostri progetti sulla base delle metriche importanti per te

Co-Sourcing
Sappiamo co-progettare e lavorare su perimetri diversi, decidiamo insieme chi fa cosa

Red Button

- Red Button è un **servizio d’intervento** per il coordinamento e l’esecuzione delle attività di gestione degli incidenti di cybersecurity.
- Rende disponibile una **squadra di specialisti** per supportarti nelle fasi di **contenimento**, **eradicazione**, **ripristino** e **analisi post-incidente** e per determinare gli opportuni miglioramenti nella gestione della tua sicurezza.

deda.tech

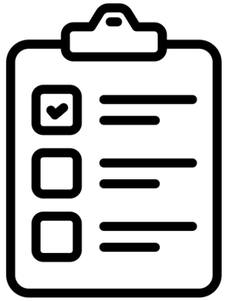
Red Button: fasi del servizio

deda.tech

Sottoscrizione

Durata contrattuale **prestabilita**

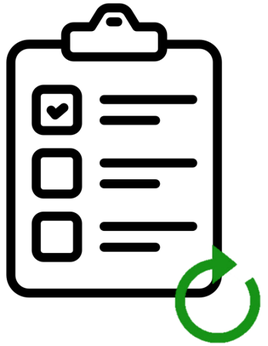
Preparazione



Assessment iniziale tecnico e organizzativo:

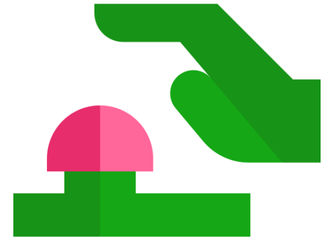
- **Piano di risposta** agli incidenti
- **Procedure di gestione** degli incidenti
- Postura e **strategie**

Esercizio



Assessment periodico: con revisione semestrale della documentazione e delle informazioni raccolte.

Emergenza

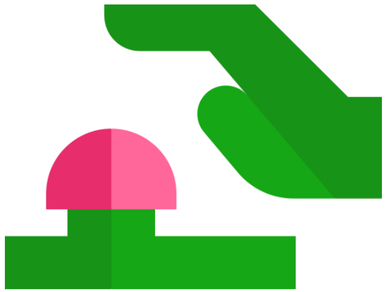


IN CASO DI INCIDENTE

- **Presa in carico**
- **Coordinamento**
- **Gestione**

Red Button: caratteristiche

deda.tech



Sottoscrizione preventiva

La sottoscrizione di un servizio a canone **mitiga** il rischio di subire un attacco cyber e **riduce i tempi** di risoluzione in caso di incidente.

Migliora la postura

Assessment e individuazione **degli ambiti di miglioramento**

Team Cyber

- Incident Response Man.
- Senior Security Manager
- Senior Incident Analyst
- Senior Forensic Analyst
- Subject Matter Expert

Organizzazione e controllo

- Definizione dei processi
- Definizione delle responsabilità
- Coordinamento delle attività di gestione dell'incidente

Negoziazione

Supporto alla negoziazione con i cyber criminali in caso di **richiesta di riscatto**

Q&A

SECURITY SUMMIT

Security Summit

Milano 11-12-13 marzo 2025

Clusit 25 2000-2025

ASTREA

Contatti:

giorgio.digrazia@dedagroup.it
https://www.dedatech.com

Vieni a trovarci al nostro stand!