

CYBER THREAT MODELLING

TAVOLO 2 – 21 Novembre 23

Marco Lombardozzi

Pre Sales Leader







Forum Risk Management obiettivo sanità 9 salute

21-24 NOVEMBRE 2023 **AREZZO** FIERE E CONGRESSI

A form of risk assessment that models aspects of the attack and defense sides of a logical entity, such as a piece of data, an application, a host, a system, or an environment NIST SP 800-53 Rev. 5

5. È possibile quantificare il 1.Individuazione beneficio atteso di una (o più) attività 1. Al contesto IT si applicano delle minacce e minacce specifiche che devono di mitigazione in termini di riduzione valutazione essere prese in considerazione dei rischi e comparare il trade-off delle insieme alle minacce comuni costi benefici di diverse strategie di probabilità mitigazione 5. Valutazione 2.Individuazione dei rischi degli impatti residui associati alle minacce (dopo la individuate mitigazione) 2. Il danno generato dal manifestarsi di una minaccia non è universale, dipende dal valore delle informazioni trattate e dalla criticità dei servizi impattati 4. Inserire un controllo di sicurezza 3. Valutazione 4.Individuazione non è sempre l'unica strategia di dei rischi 3. Valutare inizialmente i rischi senza mitigazione del rischio. Alcune volte prioritizzazzione inerenti prendere in considerazione le è possibile trasferire un rischio ad delle attività di contromisure presenti ci permette di (senza mitigazione una terza parte o evitarlo. mitigazione) valutare la reale priorità degli interventi di sicurezza









Una classificazione delle tattiche associate agli attacchi informatici e relative tecniche viene fornita dal MITRE Att&ck per tre tipologie di contesto: Enterprise; Mobile e Industrial Control Systems (ICS).

ATT&CK®

Reconnaissance

Exfiltration

Discovery

Lateral Movement

Resource Development

Persistence

Collection

Credential Access

Initial Access

Privilege Escalation Command and Control

Defense Evasion

Impact











Definizione Glossario CSRC del NIST (SP 800-53): <u>Vulnerability</u>

Weakness in an information system, system security procedures, internal controls,
or implementation that could be exploited by a threat source.

Nell'ambito della sicurezza informatica possiamo definire due macrocategorie di vulnerabilità:

- <u>Vulnerabilità non note (0 day):</u> Vulnerabilità non espressamente note al proprietario del software (e.g. vendor, sviluppatore) e di conseguenza non rese pubbliche;
- <u>Vulnerabilità note:</u> Vulnerabilità pubblicamente documentate per cui il proprietario del software ha (o sta sviluppando) una patch correttiva da mettere a disposizione degli utilizzatori del software (e.g tramite aggiornamento).











