MISURE OPERATIVE PER LA MITIGAZIONE DEL RISCHIO

UNICA
UNIVERSITÀ
DEGLI STUDI
DI CAGLIARI

IL RISCHIO INFORMATICO

Gestire i rischi richiede *misure* e *stime*

Il dominio *cyber* è costituito da elementi immateriali che portano facilmente a *sottostimare*/*minimizzare* o *sovrastimare*

Difficoltà
- individuare i punti deboli degli strumenti informatici
- stimarne le conseguenze nel mondo reale

UN CASO RECENTE: MOVEit DATA BREACH

MOVEit is a file transfer platform made by Progress Software Corporation. The platform is used by thousands of governments, financial institutions and other public and private sector bodies all around the world to send and receive information.

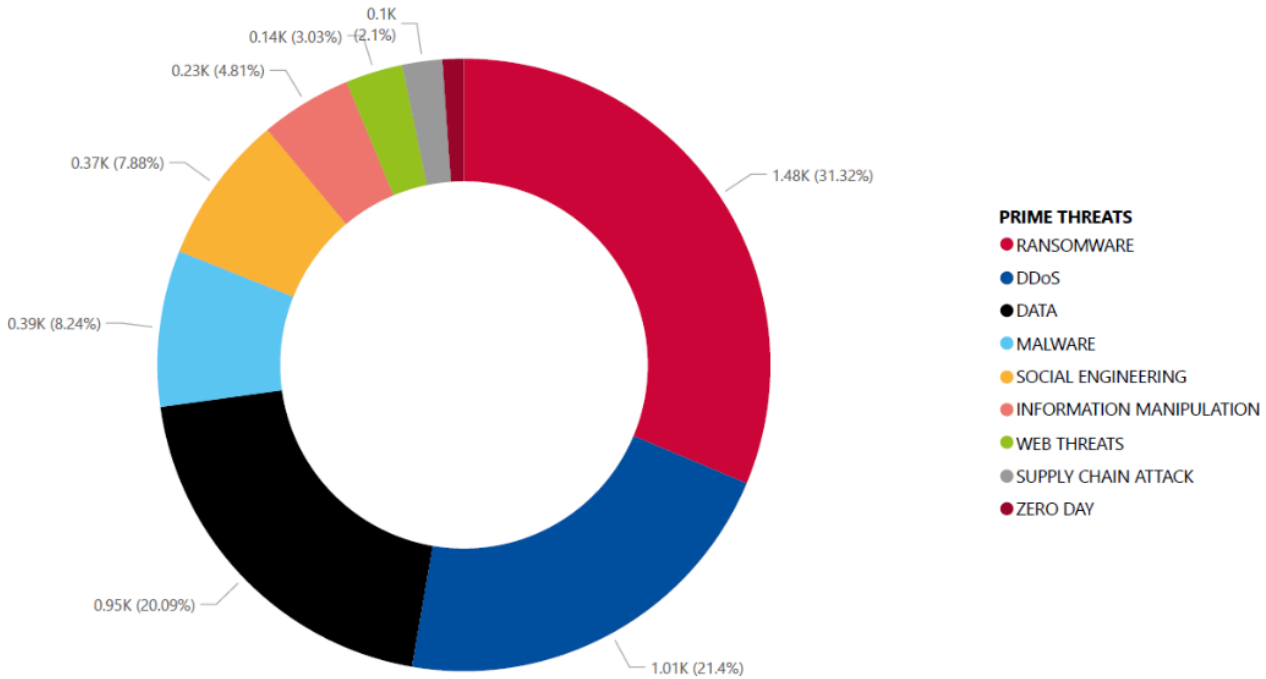
In late May 2023, data started to be transferred from hundreds of MOVEit deployments, however, these were not normal file transfers initiated by legitimate users. MOVEit had been hacked and the data was being stolen by a ransomware operation called Cl0p.

The current tally of organizations and individuals known to have been impacted by this incident is shown below. The data is sourced from state breach notifications, SEC filings, other public disclosures, as well as Cl0p's website, and is current as of November 24, 2023.

Organizations:	2,636
Individuals:	83,299,773

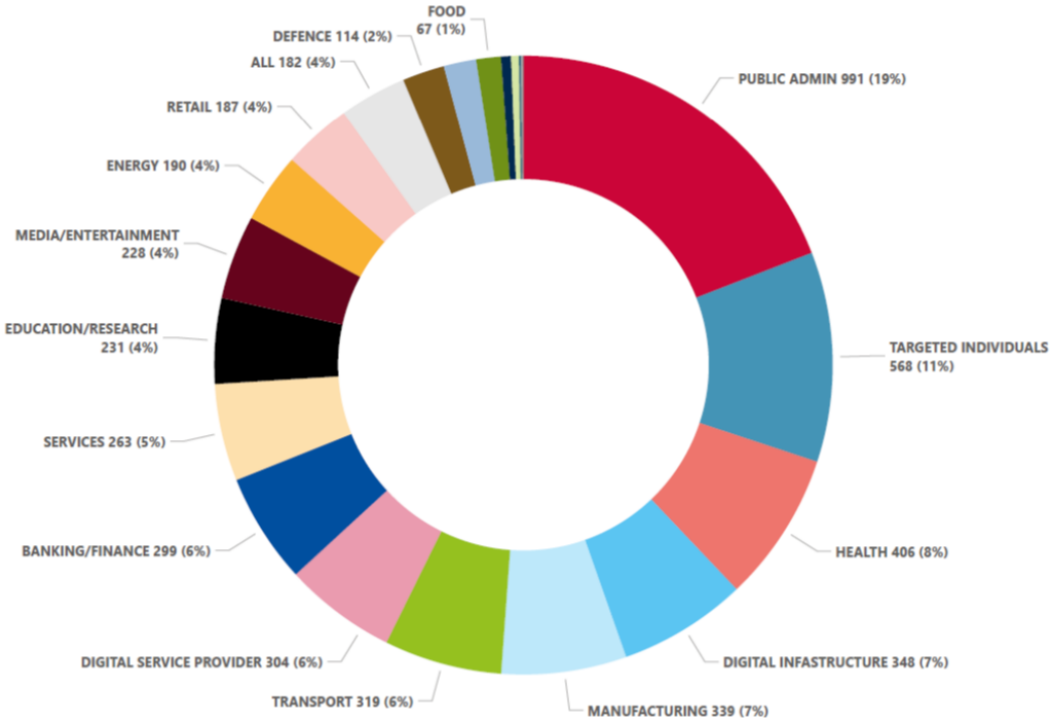
https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/

CYBERSICUREZZA



ENISA – Threat Landscape 2023

SETTORI A RISCHIO



Nessuno è esentato dalla valutazione del rischio cyber

La complessa interconnessione fra i sistemi
e la sfumatura dei contorni fra *personale* e *aziendale*

richiede una analisi mirata e dettagliata

ENISA – Threat Landscape 2023

STRUMENTI A DISPOSIZIONE

Cataloghi

CVE – Common Vulnerabilities and Exposure. 217.773 vulnerabilità

CWE – Common Weaknesses Enumeration 934 *punti di debolezza*

ATT&CK – Knowledge base of adversary tactics and techniques

Enterprise: 201 Techniques, 424 Sub-Techniques, 648 Pieces of Software, 43 Mitigations

Mobile: 72 Techniques, 42 Sub-Techniques, 108 Pieces of Software, 12 Mitigations

ICS: 81 Techniques, 13 Groups, 21 Pieces of Software, 52 Mitigations

NON SI PUÒ IMPROVVISARE

Controllo degli accessi, crittografia, aggiornamenti, monitoraggio…

Da dove iniziare?

Fase di PLAN deve essere condotta con estrema accuratezza affinché il «DO» mitighi in modo significativo il rischio

FRAMEWORK DI CYBERSICUREZZA

Le misure di

PROTEZIONE

RILEVAZIONE

RISPOSTA

RIPRISTINO

devono essere calibrate sulla specifica organizzazione

Centralità della prima fase: **IDENTIFY**

THREAT MODELING

[Application] Threat Modeling

– a **strategic** process aimed at considering

– **possible attack scenarios** and **vulnerabilities**

– within **a proposed or existing application environment**

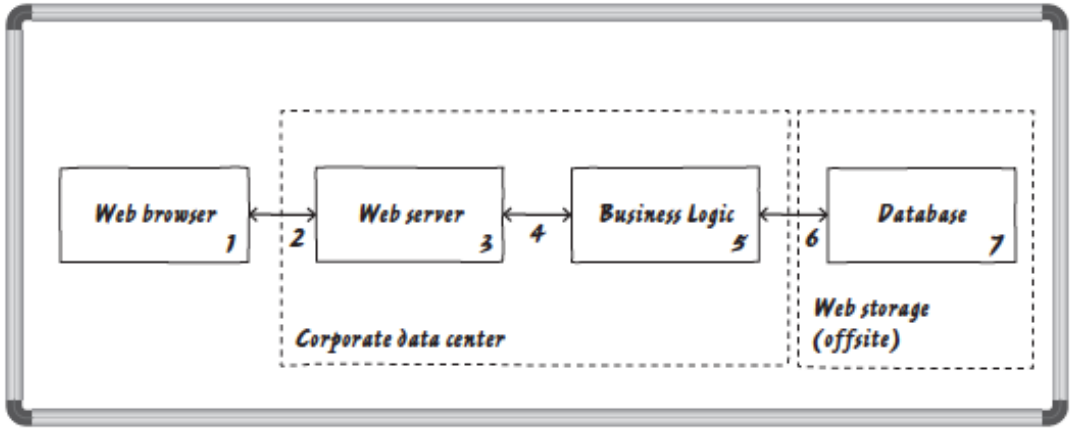
– for the purpose of clearly **identifying risk** and **impact levels**

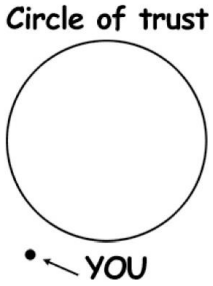
Tony UcedaVelez and Marco M. Morana, Risk Centric Threat Modeling, 2015

UN MODELLO DEL SISTEMA CYBER-FISICO

Attori coinvolti, procedure, attrezzature (fisiche e immateriali), per perseguire **gli obiettivi dell'organizzazione**

Identificazione dei **Perimetri della Fiducia**





TRADIRE LE RELAZIONI DI FIDUCIA

MINACCIA	FIDUCIA
Spoofing	Autenticazione
Tampering	Integrità
Repudiation	Non Ripudio
Information Disclosure	Riservatezza
Denial of Service	Disponibilità
Elevation of Privilege	Autorizzazione

STRIDE

Sviluppata da Microsoft a partire dal 2002

Adottata da Microsoft dal 2004 nello sviluppo dei loro prodotti

Ampia diffusione in molti altri contesti dopo la diffusione pubblica nel 2008.

COME MITIGARE EFFICACEMENTE IL RISCHIO?

Individuazione delle possibili **minacce** **specifiche**

- Riduzione del numero e complessità delle attività

Attribuzione di **valore** ai diversi componenti del sistema

- Stima delle **conseguenze** di attacchi **inclusi effetti a cascata**

Assegnazione di **priorità** in base all'**impatto**

STIMARE L'IMPATTO

Attività ancora poco diffusa, sia a livello operativo, sia nei lavori di ricerca

Impatto tecnico: quanto **è facile sfruttare** una determinata vulnerabilità per raggiungere un obiettivo?

Quali le **conseguenze**?

Impatto operativo: conseguenze su **produzione** o **erogazione** servizi

cause legali

reputazione

CIS CONTROLS

Linee guida per la mitigazione del rischio

Tre livelli di controlli in base alla complessità della realtà da mettere in sicurezza

18 aree di controllo

Inventario risorse	Gestione dei log	Formazione
Protezione dei dati	Email e Web	Fornitori di servizi
Configurazioni	Malware	Applicazioni
Gestione Account e Accessi	Recupero dati	Gestione incidenti
Gestione Vulnerabilità	Sicurezza Rete	Test di penetrazione

MONITORAGGIO CONTINUO

La protezione efficace richiede il **monitoraggio continuo** dei sistemi

- per rilevare **anomalie** riconducibili a **minacce**
- per segnalare componenti che hanno necessità di **aggiornamento**

Essenziale individuare **cosa** monitorare e **come** monitorare

- correlando con le basi di conoscenza sulle minacce informatiche

LINEE DI EVOLUZIONE PER LA CYBERSICUREZZA

Digitalizzazione crescente

Nuove tecnologie

Attacchi sofisticati che *evadono* i sistemi di monitoraggio

DIGITALIZZAZIONE

Un numero sempre maggiore di settori della vita personale, sociale, produttiva, pubblica amministrazione

Obiettivi

Migliorare la qualità della vita, sia a livello personale che sociale

Migliorare l'impatto sull'ambiente

La complessità delle interazioni cyber e cyber-fisiche è causa dell'aumento dei potenziali punti deboli che un avversario potrebbe sfruttare

NUOVE TECNOLOGIE

Nuove tecnologie vengono spesso commercializzate senza una adeguata valutazione dei punti deboli

Le difficoltà nella progettazione ed esecuzione di test esaustivi non devono diventare un alibi

L'introduzione di nuove tecnologie deve essere preceduta dalla valutazione del rischio per lo specifico contesto aziendale identificando i punti deboli e il loro impatto

SOFISTICAZIONE DELLE MINACCE

Attacchi informatici eseguiti in modo da essere simile ad applicazioni di uso comune

- Attacchi suddivisi in fasi successive ciascuna apparentemente innocua
- Parte del contenuto dannoso nascosto in contenuti multimediali
- Uso di tecniche di offuscamento

La ricerca scientifica sviluppa continuamente
strumenti avanzati in grado di rilevare le nuove tipologie di minacce

CONCLUSIONE

Gli attaccanti scelgono il bersaglio di minor costo per massimizzare l'impatto

- Tecnologie di base
- Tecnologie specifiche del settore aziendale

È più facile per un attaccante…

- Cercare una vulnerabilità nascosta in un componente specifico…
- …o sfruttare una vulnerabilità nota non gestita correttamente?