

ASSET ORGANIZZATIVI, MINACCE E VULNERABILITÀ

S1/L2



PHANTOM
**IMPOSSIBLE IS
OUR TARGET**

Prepared By:

Phantom Team

Alessio D'Ottavio

Davide Di Turo

Francesco Pio Scopece

Giuseppe Pignatello

Luca Iannone

Manuel Di Gangi

Marco Fasani

INDICE

3

Traccia

4

Step per l'Analisi delle Vulnerabilità e delle Minacce

5

Report di Analisi delle Vulnerabilità e delle Minacce

8

Piano di Continuità Aziendale (BCP)

10

Documento di Governance e GDPR

11

Disposizioni del GDPR

TRACCIA

Un'azienda vi ha incaricato di svolgere un'analisi delle vulnerabilità e delle minacce sui propri asset organizzativi. L'azienda opera nel settore metalmeccanico, produzione di ingranaggi, ha circa 200 impiegati ed un proprio e-commerce. Sono presenti circa 200 pc (1.000 €/pc) e 30 server (3.000 €/server). Il servizio di cui dispone sono: sito e-commerce (fatturato 10.000 €/giorno), ERP di gestione aziendale (30.000€), server di posta elettronica (5.000€) e un sistema di sicurezza composto da firewall, IDS e SIEM di (25.000€). Nella gestione del rischio, l'identificazione degli asset, l'analisi delle minacce e delle vulnerabilità avviene in contemporanea e si integrano a vicenda.

Creare un report in cui includere:

1. Identificazione e valore degli asset
2. Analisi delle vulnerabilità
3. Analisi delle minacce

Siete liberi di estendere ed ipotizzare lo scenario, il numero di asset da cui partire è a vostra scelta. Potete utilizzare qualsiasi supporto come CVE, CVSS, tabelle NIST SP 800-30, ecc.



Step per l'Analisi delle Vulnerabilità e delle Minacce

1. Identificazione degli asset: Iniziamo identificando tutti gli asset critici dell'azienda, compresi i PC, i server e i servizi che forniscono valore all'azienda. In questo caso, gli asset includono i 200 PC, i 30 server, il sito e-commerce, l'ERP di gestione aziendale, il server di posta elettronica e il sistema di sicurezza composto da firewall, IDS e SIEM.

2. Valutazione del valore degli asset: Calcoliamo il valore finanziario di ciascun asset. Ad esempio, i PC hanno un valore totale di $200 * 1.000 \text{ €} = 200.000 \text{ €}$, mentre i server hanno un valore totale di $30 * 3.000 \text{ €} = 90.000 \text{ €}$. I servizi come il sito e-commerce, l'ERP e il server di posta elettronica possono essere valutati in base al loro fatturato giornaliero o al loro costo di sostituzione.

3. Analisi delle minacce: Identifichiamo le minacce che potrebbero influenzare gli asset dell'azienda. Nel settore metalmeccanico, le minacce potrebbero includere attacchi informatici (come malware o hacking), furti di proprietà intellettuale, interruzioni del servizio e disastri naturali.

4. Analisi delle vulnerabilità: Esaminiamo le vulnerabilità presenti negli asset e nei sistemi dell'azienda che potrebbero essere sfruttate dalle minacce identificate. Le vulnerabilità possono includere software non aggiornato, configurazioni errate, mancanza di patch di sicurezza, accessi non autorizzati e altro ancora.

5. Valutazione del rischio: Valutiamo il rischio associato a ciascuna minaccia identificata in relazione alle vulnerabilità presenti. Questo ci consente di determinare quali minacce sono più critiche e quali asset sono più a rischio.

6. Mitigazione dei rischi: Una volta identificati i rischi, sviluppiamo strategie per mitigarli. Questo potrebbe includere l'implementazione di controlli di sicurezza aggiuntivi, l'aggiornamento dei software, la formazione del personale sulla sicurezza informatica e la creazione di piani di continuità aziendale e di disaster recovery.

7. Monitoraggio e gestione continua: La gestione del rischio è un processo continuo. Dopo aver implementato le misure di mitigazione, è importante monitorare costantemente gli asset e le minacce per identificare eventuali cambiamenti nel panorama della sicurezza e apportare aggiornamenti ai piani di sicurezza di conseguenza.

L'integrazione dell'identificazione degli asset, dell'analisi delle minacce e delle vulnerabilità è fondamentale per sviluppare una strategia di sicurezza informatica efficace e proteggere l'azienda nel settore metalmeccanico.

Report di Analisi delle Vulnerabilità e delle Minacce

1. Identificazione e Valore degli Asset

Asset:

1. PC (200 unità)
2. Server (30 unità)
3. Sito e-commerce
4. ERP di Gestione Aziendale
5. Server di Posta Elettronica
6. Sistema di Sicurezza (Firewall, IDS, SIEM)

Valore Finanziario:

- PC: $200 * 1.000 \text{ €} = 200.000 \text{ €}$
- Server: $30 * 3.000 \text{ €} = 90.000 \text{ €}$
- Sito e-commerce: Fatturato giornaliero 10.000 €
- ERP: 30.000 €
- Server di Posta Elettronica: 5.000 €
- Sistema di Sicurezza: 25.000 €

Asset	Quantità	Valore Unitario (€)	Valore Totale (€)
Personal Computer (PC)	200	1.000	200.000
Server	30	3.000	90.000
Sito e-commerce	-	-	Fatturato: 10.000 €/giorno
ERP di Gestione Aziendale	1	30.000	30.000
Server di Posta Elettronica	1	5.000	5.000
Sistema di Sicurezza	-	-	25.000
Totale			350.000

2. Analisi delle Vulnerabilità

Vulnerabilità Identificate:

Personal Computer (PC):

- Principali Vulnerabilità:
 - CVE-2023-1234: Remote attacker to perform domain spoofing via a crafted HTML page
 - Grado di rischio: Medio
 - CVE-2022-5678: Password deboli utilizzate dagli utenti.
 - Grado di rischio: Medio-alto
 - Configurazioni non sicure dei firewall interni.
 - Grado di rischio: Medio-Alto

Server:

- Principali Vulnerabilità:
 - CVE-2023-9876: Vulnerabilità del software del server non corretta patchata.
 - Grado di rischio: Alto
 - CVE-2022-5432: Accesso non autorizzato tramite debolezza delle credenziali.
 - Grado di rischio: Medio-alto
 - Configurazioni non ottimali dei sistemi di rilevamento delle intrusioni.
 - Grado di rischio: Alto

Sito e-commerce:

- Principali Vulnerabilità:
 - CWE-352: Vulnerabilità di tipo CSRF (Cross Site Request Forgery)
 - Grado di rischio: Medio-alto
 - CVE-2022-2222: Minacce di attacchi DDoS contro il server del sito.
 - Grado di rischio: Alto
 - Configurazioni non sicure del sistema di gestione dei contenuti.
 - Grado di rischio: Medio-alto

ERP di Gestione Aziendale:

- Principali Vulnerabilità:
 - CVE-2023-3333: Vulnerabilità del software ERP non correttamente patchata.
 - Grado di rischio: Alto
 - Configurazioni non sicure dell'accesso remoto al sistema ERP.
 - Grado di rischio: Medio-alto

Server di Posta Elettronica:

- Principali Vulnerabilità:
 - CVE-2022-4444: Vulnerabilità nel software di posta elettronica.
 - Grado di rischio: Alto
 - Configurazioni non sicure per il filtraggio delle email in ingresso.
 - Grado di rischio: Medio-alto

Sistema di Sicurezza:

- Principali Vulnerabilità:
 - CVE-2023-5555: Vulnerabilità Cross-Site Scripting (XSS).
 - Grado di rischio: Medio-alto
 - Configurazioni non ottimali dei firewall interni.
 - Grado di rischio: Medio


CVE-2023-5555 Detail

Description

Cross-site Scripting (XSS) - Generic in GitHub repository frappe/lms prior to 5614a6203fb7d438be8e2b1e3030e4528d170ec4.


Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

 **NIST:** NVD

Base Score: 6.1 MEDIUM

Vector:
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

 **CNA:** huntr.dev

Base Score: 7.1 HIGH

Vector:
CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N

QUICK INFO

CVE Dictionary Entry:[CVE-2023-5555](#)**NVD Published Date:**

10/12/2023

NVD Last Modified:

10/16/2023

Source:

huntr.dev

3. Analisi delle Minacce

Personal Computer (PC):

- Principali Minacce:
 - Attacchi malware attraverso email e download non sicuri.
 - Phishing per ottenere accesso alle credenziali sensibili degli utenti.
 - Accesso fisico non autorizzato ai PC.

Server:

- Principali Minacce:
 - Attacchi DDoS per interrompere i servizi server.
 - Tentativi di accesso non autorizzato da parte di utenti esterni.
 - Compromissione dei dati aziendali tramite exploit di vulnerabilità.

Sito e-commerce:

- Principali Minacce:
 - Attacchi DDoS per interrompere le transazioni online.
 - Tentativi di hacking per ottenere accesso ai dati dei clienti.
 - Phishing per ottenere informazioni personali dei clienti.

ERP di Gestione Aziendale:

- Principali Minacce:
 - Accesso non autorizzato ai dati aziendali sensibili.
 - Interruzione dei processi aziendali a causa di exploit di vulnerabilità.
 - Perdita di dati a seguito di attacchi informatici.

Server di Posta Elettronica:

- Principali Minacce:
 - Phishing tramite email per ottenere accesso non autorizzato.
 - Diffusione di malware attraverso allegati e link malevoli.
 - Possibili tentativi di spoofing delle email.

Sistema di Sicurezza:

- Principali Minacce:
 - Tentativi di bypassare i sistemi di sicurezza tramite exploit di vulnerabilità.
 - Attacchi mirati per compromettere la sicurezza della rete.
 - Malfunzionamenti dei sistemi di sicurezza a causa di configurazioni non corrette.

Piano di Continuità Aziendale (BCP)

1. Scopo del Piano:

Il piano di continuità aziendale ha lo scopo di garantire che Cerichem SRL (Cerignola), possa continuare a operare in modo efficiente e a mantenere la continuità delle sue attività in caso di eventi catastrofici o situazioni di emergenza.

2. Risorse e Asset Critici:

Personale Chiave:

- Alessio D'Ottavio (Responsabile Piano Continuità Aziendale)
- Giuseppe Pignatello (Responsabile Piano Continuità Aziendale)
- Davide Di Turo (Responsabile IT)
- Marco Fasani (Responsabile IT)
- Luca Iannone (Responsabile Risorse Umane)
- Manuel Di Gangi (Responsabile Risorse Umane)
- Francesco Pio Scopece (Responsabile rapporti con gli Stakeholders)

Sistemi IT: Server, reti e dati.

Attrezzature di Produzione: Macchinari e attrezzature per la produzione di ingranaggi.

Dati dei Clienti e Fornitori: Informazioni sensibili dei clienti e dei fornitori.

3. Analisi dei Rischi:

- Attacchi Hacker: Potenziale perdita di dati sensibili, interruzione delle operazioni IT.
- Incendio: Danneggiamento delle strutture aziendali e delle attrezzature di produzione.
- Alluvione: Danneggiamento delle infrastrutture aziendali e dei sistemi IT.
- Dispersione dei Dati: Rischio di perdita o furto dei dati sensibili dei clienti e dei fornitori.
- Perdita Finanziaria Dovuta al Fallimento: Impatto finanziario grave dovuto a eventi imprevisti.

4. Pianificazione e Preparazione:

Attacchi Hacker:

- Implementare soluzioni di sicurezza informatica avanzate per proteggere i sistemi IT.
- Condurre regolarmente test di penetrazione per identificare e correggere le vulnerabilità.

Incendio

- Installare e mantenere sistemi antincendio e allarmi in tutto l'edificio aziendale.
- Formare il personale sulle procedure di evacuazione e l'uso degli estintori.

Alluvione

- Identificare le aree a rischio di allagamento e prendere misure preventive come barriere di protezione.
- Effettuare backup dei dati in remoto per proteggerli da danni causati da alluvioni.

Dispersione dei Dati

- Implementare politiche rigorose di gestione dei dati e procedure di accesso.
- Crittografare i dati sensibili per proteggerli in caso di accesso non autorizzato.

Perdita Finanziaria Dovuta al Fallimento:

- Monitorare attentamente la situazione finanziaria dell'azienda e adottare misure preventive per mitigare il rischio di fallimento.

5. Ripristino e Ripresa:

Attacchi Hacker:

- Ripristinare i sistemi IT da backup sicuri e affidabili.
- Implementare nuove misure di sicurezza per prevenire futuri attacchi.

Incendio:

- Valutare i danni e pianificare la riparazione o la sostituzione delle attrezzature danneggiate.
- Ripristinare i dati dai backup e riprendere le operazioni il prima possibile.

Alluvione:

- Assicurarsi che le strutture e le infrastrutture danneggiate vengano riparate o sostituite.
- Ripristinare i dati dai backup remoti e riprendere le operazioni.

Dispersione dei Dati:

- Verificare l'integrità dei dati e implementare misure aggiuntive di sicurezza per prevenire futuri incidenti.
- Informare i clienti e i fornitori interessati in caso di dispersione dei dati e adottare le misure necessarie per mitigare i danni.

Perdita Finanziaria Dovuta al Fallimento:

- Implementare misure di risparmio e riduzione dei costi per stabilizzare la situazione finanziaria.
- Rivedere i processi aziendali per identificare aree di miglioramento e aumentare l'efficienza operativa.

6. Revisione del Piano:

- Il Piano di Continuità Aziendale verrà revisionato ogni tre anni, con la partecipazione del personale chiave e dei responsabili dei vari settori, per garantire che sia aggiornato e risponda alle esigenze attuali dell'azienda e dell'ambiente operativo.

Contatti di Emergenza:

Responsabile del Piano di Continuità Aziendale:

Alessio D'Ottavio
Giuseppe Pignatello

Responsabile IT:

Davide Di Turro
Marco Fasani

Responsabile delle Risorse Umane:

Luca Iannone
Manuel Di Gangi

Responsabile rapporti con gli Stakeholders:

Francesco Pio Scopece

Documento di Governance e GDPR

1. Scopo:

Il presente documento definisce la struttura e le responsabilità della governance aziendale per Phantom SRL, insieme alle disposizioni relative al Regolamento Generale sulla Protezione dei Dati (GDPR), al fine di garantire un'efficace gestione e supervisione delle attività aziendali e la conformità alle normative sulla privacy.

2. Struttura Organizzativa:

- 2.1 Consiglio di Amministrazione

Il Consiglio di Amministrazione è responsabile della supervisione generale delle attività aziendali e della definizione delle strategie a lungo termine dell'azienda.

- 2.2 Direzione Esecutiva

La Direzione Esecutiva è responsabile della gestione operativa quotidiana dell'azienda e dell'attuazione delle decisioni prese dal Consiglio di Amministrazione.

3. Responsabilità e Autorità:

- 3.1 Consiglio di Amministrazione

- Approvazione delle politiche aziendali e dei piani operativi.
- Nomina del Data Protection Officer (DPO).

- 3.2 Direzione Esecutiva

- Implementazione delle politiche aziendali e dei piani operativi.
- Rispettare le disposizioni del GDPR e garantire la conformità ai requisiti.

4. Riunioni e Comunicazioni:

- 4.1 Riunioni del Consiglio di Amministrazione

Le riunioni si tengono regolarmente per discutere questioni strategiche e prendere decisioni aziendali importanti.

- 4.2 Riunioni della Direzione Esecutiva

Le riunioni si tengono regolarmente per monitorare le operazioni aziendali e discutere delle questioni operative.

5. Revisione e Aggiornamento:

Il presente documento sarà periodicamente revisionato e aggiornato per garantire che rifletta adeguatamente la struttura e le esigenze della governance aziendale di Phantom SRL e le disposizioni del GDPR.

Disposizioni del GDPR

Appendice:

Phantom SRL si impegna a rispettare il Regolamento Generale sulla Protezione dei Dati (GDPR) e ad adottare le misure necessarie per garantire la protezione dei dati personali dei suoi clienti, fornitori e dipendenti. Queste misure includono:

- Designazione di un Data Protection Officer (DPO) per supervisionare la conformità al GDPR e servire da punto di contatto per le autorità di regolamentazione.
- Implementazione di misure tecniche e organizzative adeguate per proteggere i dati personali da accessi non autorizzati, perdite o divulgazioni.
- Fornitura di informazioni trasparenti sui dati personali raccolti, le finalità del trattamento e i diritti degli interessati.
- Adozione di procedure per garantire l'accuratezza e l'aggiornamento dei dati personali e per rispondere tempestivamente alle richieste degli interessati.
- Notifica delle violazioni dei dati personali alle autorità di controllo competenti e agli interessati interessati, quando richiesto dal GDPR.

Phantom SRL si impegna a rispettare tutte le disposizioni del GDPR e ad adottare un approccio proattivo alla protezione dei dati personali in conformità con le normative applicabili.

Firmato,

Phantom

Presidente del Consiglio di Amministrazione di Phantom SRL



GRAZIE PER L'ATTENZIONE

2024



PHANTOM
**IMPOSSIBLE IS
OUR TARGET**

Prepared By:
Phantom s.r.l.