Davide Andreozzi

BCC – Risk Management

S01 – L02

Agenda

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

1) Identificazione e valore degli asset

Asset	Value	Impact (0-10)	Costi
PC	200.000	5	15.000
Server	90.000	7	22.000
E-commerce	3.650.000	10	75.000
SW ERP	30.000	7	2.000
Server SMTP	5000	8	750
Sistema di sicurezza rete	25.000	8	3.400

2) Analisi delle vulnerabilità

Asset	Vulnerabilità	Fonte
PC	I pc non dispongono di credenziali forti per l'autenticazione, i dipendenti non sono formati a sufficienza contro il phishing	Penetration Test
Server	I server si trovano in una stanza adiacente alla zona di produzione con elevati rischi legati alla temperatura e agli incendi che potrebbero avere fonte dalla zona di produzione	Interviste personale, mappa dell'azienda
E-commerce	Il server e-commerce è potenzialmente vulnerabile ad attacchi DDoS, i backup sono effettuati mensilmente	Scansione interna
Server SMTP	Credenziali per l'accesso deboli	Interviste personale, Penetration test
Sistema di sicurezza rete	Monitoraggio della rete non presente, settaggio dispositivi di sicurezza mediocre	Penetration Test

3) Analisi delle minacce

Asset	Vulnerabilità	Minacce	Attori	Probabilità
PC	I pc non dispongono di credenziali forti per l'autenticazione, i dipendenti non sono formati a sufficienza contro il phishing	Rischio di Malware a seguito di un attacco phishing con buone probabilità di scalata dei privilegi	Criminali informatici	Alta
Server	I server si trovano in una stanza adiacente alla zona di produzione	Rischio di guasto o incendio alla server room dovuto alle alte temperature	Fattori naturali, Personale	Media
E-commerce	Il server e-commerce è potenzialmente vulnerabilità ad attacchi DDoS, i backup sono effettuati mensilmente.	Attacco DDoS mirato al down del server con conseguenti perdite economiche derivate da inattività e perdita dati	Criminali informatici / Competitor aziendali / Personale interno	Medio-Alta
Server SMTP	Credenziali per l'accesso deboli	Attacco di brute force	Criminali informatici	Medio-Bassa
Sistema di sicurezza rete	Monitoraggio della rete non presente, settaggio dispositivi di sicurezza mediocre	Analisi dei log assente, impossibile identificare eventuali attacchi in corso, i dispositivi risultano facilmente bypassabili	Criminali informatici / Personale interno	Media