blumatica
Software Edilizia e Sicurezza

Servizi
Cyber Security

1. VAPT (Vulnerability Assessment & Penetration Testing)
2. Monitoraggio Eventi di Sicurezza & Installazione e Configurazione
3. Computer Forensics & Incident Response

Servizi
Cyber Security

VAPT
(Vulnerability Assessment & Penetration Testing)

Le attività di Vulnerability Assessment e Penetration Test (VAPT) hanno il comune obiettivo di fornire una conoscenza dettagliata sullo stato di sicurezza dei propri sistemi informatici. In particolare, attraverso diverse fasi di analisi, effettuate simulando differenti scenari di intrusione, le metodologie adottate da Blumatica permettono di:

- verificare che le informazioni sulla rete visibili da Internet siano ridotte al minimo;
- verificare che non sia possibile ottenere accessi non autorizzati a sistemi ed informazioni;
- valutare se per un utente interno sia possibile accedere ad informazioni o ottenere privilegi per i quali non ha l'autorizzazione necessaria;
- verificare che una Web Application non contenga vulnerabilità che permettano ad un attaccante di ottenere accessi non autorizzati a dati riservati, in particolare impersonificazione di altri utenti, privilege escalation, accesso interattivo alla rete target, attacco all'utente dell'applicazione, Denial of Service.

La procedura di VAPT è suddivisa in 3 fasi:

1. **Interna**, in cui viene eseguita una simulazione di un attacco dall'interno del perimetro dell'azienda;
2. **Esterna**, in cui viene eseguita una simulazione di un attacco proveniente dall'esterno del perimetro dell'azienda utilizzando la connessione internet;
3. **Web/Applicativa**, in cui vengono testati tutti gli applicativi proprietari/conosciuti per scovare vulnerabilità di funzionamento;

La fase finale dell'attività di VAPT è la reportistica, durante la quale si forniscono all'azienda ed alle persone preposte i risultati ottenuti. E' in tale fase che è possibile sottolineare gli aspetti del sistema considerati sicuri e quelli per cui vi è bisogno di migliorare la sicurezza

Servizi
Cyber Security

Monitoraggio
Eventi di Sicurezza & Installazione/Configurazione

Tra i servizi offerti da Blumatica c'è sicuramente il servizio di monitoraggio di eventi di sicurezza che consiste nel monitorare gli eventi di sicurezza provenienti dalla rete, applicativi, endpoint's e server's in modo da prevenire e/o bloccare eventuali attività anomale.
Verrà installato nella rete del cliente (e/o in cloud) un SIEM (software di monitoraggio) dal quale sarà possibile controllare tutte le attività sopra descritte.
Il SIEM sarà conforme a tutte le normative/-standard vigenti sul GDPR e gli eventi archiviati in esso saranno firmati digitalmente per comprovare l'integrità e l'autenticità del dato in esso contenuto.

Il servizio può essere erogato in 2 modalità:

- H24 (il monitoraggio verrà effettuato 7giorni su 7 h24)
- Orario base o 8x5 (il monitoraggio verrà effettuato solo nei giorni lavorativi e negli orari lavorativi del cliente, ad esempio lun-ven 9.00-18.00)

Per scenari di questo tipo Blumatica propone il **SIEM "Splunk ES (Enterprise Security)"**, servizio di rilevamento e risposta ai cyber attacchi mirati. Splunk include agent leggeri per il monitoraggio e la collezione di eventi di sicurezza su reti e server distribuiti nell'intera infrastruttura IT. I sensori monitorano le attività avviate dagli attaccanti e trasmettono tutte le informazioni al SIEM Splunk in tempo reale. Il servizio ricerca eventuali anomalie nei dati utilizzando una combinazione di tecnologie avanzate come UseCase predefiniti, l'analisi del comportamento in tempo reale, l'analisi dei Big Data e l'analisi della reputazione. La ricerca delle anomalie procede in due direzioni: **comportamenti malevoli noti e sconosciuti.**
L'uso di tipologie di analisi differenti garantisce il rilevamento degli attaccanti, anche se usano tattiche di evasione progettate per eludere metodi di rilevamento specifici. Le anomalie vengono segnalate al team di sicurezza per verificarle ed applicarne eventuali remediation.

Servizi
Cyber Security

Computer Forensics & Incident Response

Il servizio di Computer Forensic consiste nell'eseguire copie ed analisi di supporti compromessi in incidenti di sicurezza consolidati, estrarne la «root case» ed emettere un report di incident response che contenga la spiegazione dettagliata dell'incidente.

La procedura di Computer Forensic segue 4 fasi:

1. **Copia forense del dispositivo:** vengono acquisiti i dati secondo le normative vigenti, senza alcuna alterazione dei contenuti e con l'emissione di firme digitali per comprovare l'inalterabilità dei dati copiati.

2. **Data carving:** tecnica che consente di recuperare file dallo spazio non allocato di un supporto di memorizzazione di dati digitali anche quando non vi è più traccia di quel file nella tabella di allocazione, estrarre sample/file utili alle analisi dell'incidente e riscostruire lo scenario di «entry point»

3. **Report incidente:** fase in cui viene emessa la reportistica utile a riscostruire l'interno scenario di attacco/intrusione in dettaglio

4. **Remediation:** fase in cui verranno prese delle contromisure in base all'analisi dell'incidente accaduto, estrazione di IoC (Indicatori di compromissione) e/o aggiornamento delle «signature» sulle varie applicances di sicurezza e monitoraggio. La fase di remediation potrebbe prevedere in alcuni casi la bonifica degli host's/-endpoint's compromessi.

I software utilizzati da Blumatica per l'acquisizione e l'analisi forense soddisfano tutti i requisiti delle normative vigenti in ambito di privacy & computer forensic.