Your information security partner

Carta dei servizi

MISSION

La nostra mission è quella di dare supporto alle aziende nello sviluppo della propria propria infrastruttura informatica, ottimizzando i processi aziendali e proteggendo gli asset dell'organizzazione e dei propri clienti.

Crediamo fortemente nella condivisione del Know-how, nella collaborazione e nel costante sviluppo delle competenze.

ABOUT US

Backloop nasce nel 2014 su iniziativa di **Enrico Pasqualotto, CEO dell'azienda**, il quale dopo aver conseguito studi in ambito informatico ed aver maturato un'esperienza come responsabile tecnico di un'azienda veronese, decide di avviare la propria attività imprenditoriale.
Grazie alle collaborazioni e partnership con importanti realtà operanti nel settore IT, l'azienda fin da subito si trova impegnata su **progetti di ampia scala per multinazionali** operanti in svariati settori merceologici.
Backloop amplia così in poco tempo il suo team avvalendosi di **tecnici specializzati**, sviluppando costantemente **know how** e **competenze**.
Ad oggi Backloop è composta da un **team di tecnici certificati e collaboratori**, occupandosi di **consulenza ed assistenza a 360 gradi in ambito informatico**.

SERVIZI

Information Security

Infrastructure

Unified Communication

INFORMATION SECURITY

- **DARKWEB MONITORING:** Servizio che **ricerca regolarmente le informazioni relative all' azienda nei luoghi ove esse vengono scambiate**. Eseguiamo una **scansione delle risorse sul web e darkweb alla ricerca di informazioni riservate relative all'organizzazione.** Solitamente vengono rinvenute credenziali, contenuti “pastebin” contenenti informazioni aziendali, post su forum di settore e dati esposti involontariamente. Viene in seguito consegnato al cliente un **report** relativo alle evidenze rilevate ed eventuali remediation possibili.

- **VULNERABILITY ASSESSMENT:** Consiste in un insieme di attività di **scansione automatizzata del perimetro esterno o di porzioni di rete** (es. rete server o management) che permette di **individuare e classificare vulnerabilità note o configurazioni errate che potrebbero essere punti di accesso per attacchi informatici.**
  L'attività prevede i seguenti step:
  a. Scansione del perimetro
  b. Analisi manuale delle vulnerabilità rilevate e identificazione falsi positivi
  c. Creazione dei report contenente indicazioni sulle remediation
  d. Scansione del perimetro dopo l'applicazione delle remediation ed aggiornamento del report
  Software utilizzati: Qualys e AlienVault

INFORMATION SECURITY

- **TRAFFIC ANALISYS:** Servizio idoneo alla **rilevazione di malware/backdoor/traffico malevoli** a fronte di indicatori di compromissione, fornendo così intelligence in tempo reale al team di addetti alla sicurezza. Consiste nell'installazione di un **appliance che analizza il traffico di rete ed eventi generati da Active-Directory ed applicazioni** (firewall, antivirus, server). Tutti gli eventi vengono in seguito correlati in modo da identificare allarmi ed anomalie.
  Software utilizzati: Alien Vault

- **IT SECURITY OPERATION:** Servizio a canone mensile per l'**analisi di eventuali incidenti ed eventi di sicurezza generati dai software aziendali.** Vengono presi in carico segnalazioni da antivirus, firewall, active-directory, antispam, SIEM, ecc e gestite tramite workflow approvati con il cliente. Il servizio comprende supporto agli utenti finali per identificare tentativi di phishing, gestire l'eventuale perdita o furto di asset aziendali ed altre esigenze lato utente in tema di IT security. Nei workflow/playbook definiti con il cliente è inclusa la sezione di contenimento per bloccare o mitigare le minacce.

INFORMATION SECURITY

- **PATCHING MANAGEMENT:** Offriamo un **servizio di gestione degli aggiornamenti** andando periodicamente ad installare patch su sistemi Windows server e Linux. Oltre alle attività periodiche, solitamente mensili, nel caso di vulnerabilità critiche applichiamo aggiornamenti o remediation con SLA predefiniti con il cliente. Il nostro servizio SOC inoltre può anche notificare le vulnerabilità all'IT interno. L'applicazione delle patch o aggiornamenti avviene di norma tramite WSUS per i server Windows. Per server Linux possiamo usare strumenti in dotazione al cliente oppure intervenire in modo manuale. Quando possibile applichiamo le patch su un campione predefinito e nel caso non vengano rilevate anomalie l'aggiornamento diventa massivo.

INFRASTRUCTURE

- **BIG DATA & EVENT CORRELATION:** Supportiamo l'azienda nella **gestione di eventi, log e grandi moli di dati utilizzando software leader di mercato**. Ci occupiamo della gestione di tutta l'attività, dall'invio dei dati alla piattaforma di indicizzazione alla creazione di dashboard fruibili dall'enduser. L'attività svolta risolve ad esempio il problema della gestione dei log/accessi degli utenti o degli amministratori sui sistemi aziendali. I dati vengono infatti mantenuti su piattaforme con possibilità di controllo dell'integrita e della retention predefiniti. Consente inoltre di memorizzare tutte le operazioni che effettuano gli utenti sugli applicativi o file aziendali (audit log).
  Software Utilizzati: Splunk, ELK

- **ANTIVIRUS: Servizio per il deploy massimo di antivirus.** Gestiamo l'eventuale sostituzione e tuning delle impostazioni seguendo le best-practice di framework per la cyber-security. Il servizio può integrarsi con IT Security Operation per la gestione delle segnalazioni generate dai software.
  Software utilizzati: Sophos, Trendmicro

INFRASTRUCTURE

- **IT OPERATIONS:** Servizio di completa **gestione dell'infrastruttura informatica dell'azienda**. Il supporto comprende i ticket degli enduser e la manutenzione di server ed apparati. Il servizio è erogato in modalità ibrida sia onsite che remoto.

- **MONITORING:** Deploy di **strumenti per il monitoraggio dell'infrastruttura informatica, che comprende la generazione di appositi alert tramite mail.** Gli strumenti utlizzati, solitamente Zabbix, possono essere on-premises o cloud con apposite appliance presso il cliente. La padronanza dello strumento ed il know-how maturato ci permettono di effettuare personalizzazioni tramite API per rispondere ad esigenze verticali e specifiche.
  Software utilizzato: Zabbix

- **FIREWALL: Gestiamo i firewall e ci occupiamo del loro deploy** nelle seguenti modalità:
  – cloud based per infrastrutture ibride
  – perimetrali
  – interni per la segmentazione della rete
  Prodotti utilizzati: Sophos, Palo Alto Networks, Cisco ASA e PfSense

INFRASTRUCTURE

- **NETWORK ACCESS CONTROL:** L'implementazione di un NAC è parte del processo di segmentazione della rete aziendale, **la nostra soluzione basata sul prodotto PacketFence permette un'assegnazione dinamica delle VLAN in base ad utenti e gruppi di Active-Directory** senza essere legati a porte fisiche degli switch. Nel caso il dispositivo non abbia un utente associato la soluzione può utilizzare il mac-address o la tipologia di dispositivo. L'utilizzo del protocollo RADIUS nella comunicazione tra switch e server di dominio permette una gestione omogenea per i device wired (802.1x) e wireless (WPA2/3 enterprise)
  Prodotti utilizzati: PocketFence

- **ASSET MANAGEMENT: Consente di conoscere e controllare le componenti dell'infrastruttura informatica di un'azienda ed assegnare la corretta criticità ad ogni server e dispositivo.** I software che utilizziamo permettono l'inventario semi-automatizzato dei dispositivi in rete e di tutti i software installati presso gli endpoint. Quest'ultimo passaggio è fondamentale per conoscere quali software obsoleti o vulnerabili sono presenti in azienda.
  Prodotti utilizzati: Lansweeper, PDQ Deploy/Inventory.

UNIFIED COMMUNICATION

- **IP - PBX: Il servizio consiste nell' implementazione di soluzioni IP-PBX integrate con l'infrastruttura aziendale che consentono di dirottare le chiamate in entrata in base a diversi database/gestionali od alla tipologia di settore. Alcuni esempi di implementazioni:**
  - gestione di letture gas/energia elettrica tramite telefono
  - routing delle chiamate in base ad informazioni tratte dal gestionale
  - gestione di interpretariato telefonico con 3 o più partecipanti
  - gestione di appuntamenti tramite telefono
  - call center inbound / outbound

  Prodotti utilizzati: Asteriks, Cisco CallManager

- **INTEGRAZIONE MS TEAMS:** Ci occupiamo dell'integrazione del PBX VoIP on-premises con il tenant Microsoft O365, utilizzando apposite soluzioni SBC certificate. L'integrazione permette di effettuare e ricevere chiamate usando il client Teams senza altri softphone. L'utilizzo di MS Teams risulta molto agevole in quanto già installato sugli endpoint ed utilizzato quotidianamente per le comunicazioni interne.

  Prodotti utilizzati: Audiocodes, Asterisk, MS Teams

PARTNERSHIP

Crediamo fortemente nella cooperazione e condivisione del nostro know-how, per questo fin dagli esordi abbiamo instaurato collaborazioni con aziende operanti nell'ambito IT, mettendo a disposizione dei partner i nostri prodotti che vengono così integrati in soluzioni di terze parti.

QUALITÀ

QUALITÀ CERTIFICATA

Abbiamo conseguito le seguenti certificazioni al fine di garantire la qualità dei nostri servizi

CONTATTI

Backloop srl
Sede operativa: Via degli Alpini 2A,
Palazzolo di Sona (VR)
Sede legale: Via Satiro 11.
Verona (VR)

Tel: +39 045 9971269

E-mail: info@backloop.biz
Web site: www.backloop.biz

Linkedin