Security AsAServiceS

Senza Alternativa

I Portici – Torre dell'Orologio Bologna

12-10-2023

Le aziende del Gruppo MEET IT

Agenda

10,30 Introduzione e benvenuto: il gruppo MeetIT le sinergie per i servizi a voi SCAAS nel mondo che cambia

Dr. Giuseppe Mazzoli - Amministratore 3CiME Technology – Gruppo Meet IT www.3cime.com

10,45 Sophos: il servizio SOC del Gruppo MeetIT -la Security As A Service

Dr. Massimiliano Catanzaro- Sophos Italia www.sophos.it

11,15 Delinea: Il PAM Privileged Access Management: le password dei server in cassaforte e la semplificazione nella gestione dei PC

Dr. Nicola D'Ottavio– Sales Manager di Delinea www.delinea.com

11,45 Comune di Bologna: che bello e completo il nostro progetto Pam con Delinea

Dr. Stefano Mineo www.comune.bologna.it

11,50 PenTera: la base del servizio di Penetration Test Continuativo del Gruppo Meet IT dal nome P3natioN

Dr.ssa Irene Casagrande www.pentera.io

12,20 Barracuda: L'evoluzione della sicurezza scandita dai ritocchi dell'orologio della Torre

Dr. Luca Bin - Barracuda Italia www.barracuda.com

13,00 Pranzo

14,30 – 16,00 Visita alla Torre dell'Orologio – Palazzo d'Accursio – Piazza Maggiore Bologna.

2023 Un anno sulla security

- 7 febbraio con Commvault per il backup di 365 (venduto in RER – 6000 utenti)
- 14 marzo con Dynatrace e Lepida per il monitoring
- 4 maggio con tanti vendor e clienti (Air Dolomiti, Danieli, Città Metro)
- 13 giugno con Zabbix e il nostro prodotto di monitoring Cassandra
- 15 giugno con Alludo – Parallels – Awingu per lo smart working
- Tanti webinar della nostra consociata NT

La visione olistica della gestione dei dati

Cominciamo da qui: informatica per imprenditori

Quindi nel libro c'è tutto?

No, dobbiamo continuare a girare la ruota nel tempo.

Approccio olistico

Le novità del mondo che va avanti

- Come tutti sappiamo le minacce nuove ci sono e sono sempre più complicate
- Ma quali minacce?
- Poi non ci sono professionalità che ci aiutino (c'è solo il gruppo MeetIT? - Noooo)
- Ci sono difficoltà nel parlare di queste cose con il board
- Il 57% delle organizzazioni è NO CISO
- E poi bisogna rassegnarsi ad aumentare la spesa ICT in Security (oggi il 5% della spesa ICT complessiva)
- Ma spesi questi siamo a posto? No, se la sicurezza diventa un servizio!

Quali sono le minacce - vettori

- 60% derivano dalla navigazione
- 28% dalle mail
- I pirati puntano al furto delle credenziali
    I. Degli amministratori
    II. Degli utenti

Quali sono le minacce – le novità

- ChatGPT: l'intelligenza artificiale sarà utilizzata per creare malware
- Le mail di phishing: non ci saranno più errori grammaticali!
- Gli audio con la voce del boss che ti dicono di fare… un bonifico!
- I video del boss «craccati da instagram» o dai social con l'ordine di acquistare un prodotto con consegna a casa dell'hacker

Quali sono le minacce – le novità

- Le mail per esempio devono affrontare un phishing evoluto: anche il blocco dei DNS Malicious è superabile.
- I link malevoli sono hostati da domini «trusted», come Google, Microsoft, Evernote, ecc.
- Ah, dimenticavo: ad un cliente hanno attaccato e bucato l'AS/400!

I punti di arrivo

- Impersonation protection: sono tecnologie che puntano a proteggere la nostra persona ed a mitigare i furti di identità
- SOC Security Operation Center che deve proteggere:
  - Il network
  - Le mail
  - I server
  - Gli endpoint
  - I dati e applicazioni on-premise o in cloud

I punti di arrivo

- Vi annuncio due cose:
- Si può fregare l'MFA Multi Factor Authentication, con una semplice triangolazione (Man In The Middle) ad esempio per l'autenticazione su un cloud
- Le applicazioni in SAAS non sono protette!

I punti di arrivo

- Il firewall diventa un servizio cloud: per esempio per accedere alle applicazioni SAAS si deve acquistare un servizio WAF AsAService
- Per superare l'MFA dovremo arrivare all'agente Zero Trust: sentirete parlare di SASE Secure Access Service Edge

I punti di arrivo per bloccare l'ATO Attack Take Over

- Blocco dei domini malevoli o sospetti
- Blocco degli ip address malevoli o sospetti
- Blocco degli indirizzi e-mail mittenti malevoli e sospetti
- Blocco di chi ci scrive una mail per la prima volta
- Blocco
- Blocco
- E poi?!?!?

Sono sempre regole

Non ce la facciamo più: basta regole

Una soluzione INTELLIGENZA ARTIFICIALE + SERVIZIO GESTITO

SCAAS Security As A Service

Bisogna fare alcuni passi avanti

- Prendere un servizio SOC: non è più rimandabile
- Prendere un servizio PAM per mettere in cassaforte le pwd degli amministratori e mitigare il rischio di ATO
- Monitorare lo stato della nostra sicurezza, con PenTest continuativi
- Evolvere la sicurezza dei mondi SAAS ed e-mail
- Anche le applicazioni containerizzate devono essere protette e controllate (vedi nostro servizio di Container Security)

Un ultimo appunto nella scelta del SOC

- Scrivo sul mio blog: https://www.meetit.cloud/it-it/02/2023/sicurezza-dei-dati/security-operations-center-come-scegliere-il-giusto-servizio-soc/

- Allarme
- Allarme + blocco dell'attacco
- Allarme + blocco dell'attacco + remediation
- Remediation correttive
- Remediation preventive

Un ultimo appunto nella scelta del SOC

- Valutare la squadra di persone
- Valutare la copertura oraria del livello di servizio
- Valutare la copertura mondiale di un SOC: diffidate di un SOC «solo italiano» o comunque monosede
- Considerare l'inclusione a forfait delle remediation nel prezzo proposto (correttive e preventive)
- Considerare come plus la presenza di una "garanzia" contro il data breach, ossia la possibilità di avere un rimborso economico in caso di attacco andato a buon fine

Servizi a corollario ma sempre security è

- Censimento degli asset tramite Armis
- Servizio di cifratura dei data base
- Servizio di archiviazione dei dati freddi
- Penetration Test su Active Directory
- Il backup di 365 o di archiviazione Google
- Il servizio che aiuta l'help desk nel rendere autonomi gli utenti che sbagliano la password

Grazie!

Giuseppe Mazzoli, *CEO*

12/10/2023

meetit.cloud

Le aziende del Gruppo MEET IT