intuity

2019 THROUGH THE EYES OF A HACKER

I PROBLEMI DI CYBERSECURITY PIÙ SIGNIFICATIVI NELLE AZIENDE ITALIANE RACCONTATI ATTRAVERSO L'ESPERIENZA DIRETTA, ACQUISITA CON L'EROGAZIONE DEI NOSTRI SERVIZI RED TEAM E BLUE TEAM NEL CORSO DEL 2019.

CONTESTO

53 AZIENDE CLIENTI

12 RED TEAM

150 REPORT REALIZZATI

+5.500 INDIRIZZI IP ANALIZZATI

286 WEB APPLICATION ANALIZZATE

15 PHISHIG CAMPAIGN

+2.600 UTENTI RAGGIUNTI CON IL PHISHING

RISULTATI

RED TEAM

VIOLAZIONE DATI DI BUSINESS — 100%

COMPROMISSIONE DI ALMENO UN SISTEMA CRITICO — 75%

COMPROMISSIONE DI ALMENO UNA CASELLA DI POSTA C-LEVEL — 50%

PENETRATION TEST

23% SISTEMI COMPROMESSI SFRUTTANDO VULNERABILITÀ CRITICHE

WEB APPLICATION PENETRATION TEST

35% APPLICAZIONI VIOLATE SFRUTTANDO VULNERABILITÀ CRITICHE

SOCIAL ENGINEERING

SUCCESSO PHISHING

MASS PHISHING **17%**

SPEAR PHISHING **28%**

22% VOLTE IN CUI TRAMITE SPEAR PHISHING ABBIAMO OTTENUTO UN ACCESSO A DATI SENSIBILI

SUCCESSO ATTACCHI FISICI

VOLTE IN CUI SIAMO RIUSCITI AD ENTRARE IN UN'AREA RISERVATA E ABBIAMO OTTENUTO DATI SENSIBILI — **66%**

SUCCESSO IMPERSONATION TELEFONICA

VOLTE IN CUI ABBIAMO OTTENUTO LE INFORMAZIONI RICHIESTE — **50%**

SUCCESSO DEL BAITING

VOLTE IN CUI È STATA INSERITA LA CHIAVE USB ED ESEGUITO IL MALWARE — **30%**

PASSWORD

+85.770 PASSWORD HASH OTTENUTI

+13.500 PASSWORD HASH "CRACCATI"

210 SISTEMI CON PASSWORD DI DEFAULT IDENTIFICATI

+4000 PASSWORD DEBOLI RILEVATE

+87 CASI VERIFICATI IN CUI L'UTENTE HA MODIFICATO LA PASSWORD IN MODO PREVEDIBILE

VALUTAZIONI QUALITATIVE

MAGGIORI VULNERABILITÀ CRITICHE RILEVATE

NETWORK

- ETERNALBLUE
- DEFAULT/BLANK CREDENTIAL
- SMB SIGNING DISABLED
- RDP BLUEKEEP
- CIFS NULL SESSION

MAGGIORI VULNERABILITÀ CRITICHE RILEVATE

WEB

- SQL INJECTION
- UN RESTRICTED FILE UPLOAD
- BROKEN ACCESS CONTROL
- PATH TRAVERSAL
- XSS

MAGGIORI VULNERABILITÀ CRITICHE RILEVATE

GOVERNACE

- MANCANZA DI SEGREGAZIONE
- MANCANZA DI UN ADEGUATO PROCESSO DI PATCHING
- MANCANZA DI FORMAZIONE CAPILLARE
- OBSOLESCENZA DEI SISTEMI OPERATIVI
- INADEGUATEZZA DEI SISTEMI ANTISPAM
- SCARSO IMPIEGO DI "STRONG AUTHENTICATION"
- ENDPOINT PROTECTION INEFFICIENTE

DIFESA

4/12 NUMERO DI RED TEAM IN CUI LE NOSTRE ATTIVITÀ SONO STATE IDENTIFICATE DA UN SISTEMA TECNOLOGICO

5/12 NUMERO DI RED TEAM IN CUI LE NOSTRE ATTIVITÀ SONO STATE IDENTIFICATE DA UN ESSERE UMANO

CONSIDERAZIONI FINALI

1) Attaccare un'organizzazione nella sua interezza e complessità (Red Team) considerando tecnologia, struttura e persone, garantisce quasi sempre che l'attacco vada a buon fine, spesso con danni di business potenziali enormi.

Le aziende trascurano questo aspetto e non sempre hanno una percezione corretta dei rischi e degli impatti di un attacco informatico.
Proprio per questa reale facilità di avere successo il cybercrime sta sistematicamente violando aziende di ogni ordine e grado.
L'obiezione ancora frequente "ma chi vuoi che abbia interesse ad attaccare noi? Non siamo mica una banca" denota una pericolosa e distorta visione della situazione.

2) Da un punto di vista infrastrutturale le applicazioni web risultano essere un drammatico punto debole, sempre più spesso sviluppate senza alcuna attenzione al tema della sicurezza.

Chi commissiona attività di Penetration Test si limita spesso all'aspetto network o sistemistico, le applicazioni web invece sono raramente incluse in questa analisi, per motivi economici o per scarsa consapevolezza del rischio ad esse associato.

3) Il phishing rimane ancora uno strumento ad altissima percentuale di successo: un fenomeno che sta maturando nelle tecniche e nella capacità di essere credibile.

La formazione è vista più come un aspetto di conformità normativa che come scelta strategica per la sicurezza aziendale.
Ancora presente è un'anacronistica debolezza dei sistemi antispam, spesso assenti o mal configurati.

4) Anche le più tradizionali Best Practice sulla sicurezza informatica trovano scarsa applicazione.

Segregazione, patch management, assessment periodici da sempre sono tra le buone pratiche e considerate misure minime per una corretta gestione della sicurezza informatica, raramente però trovano adeguata applicazione.