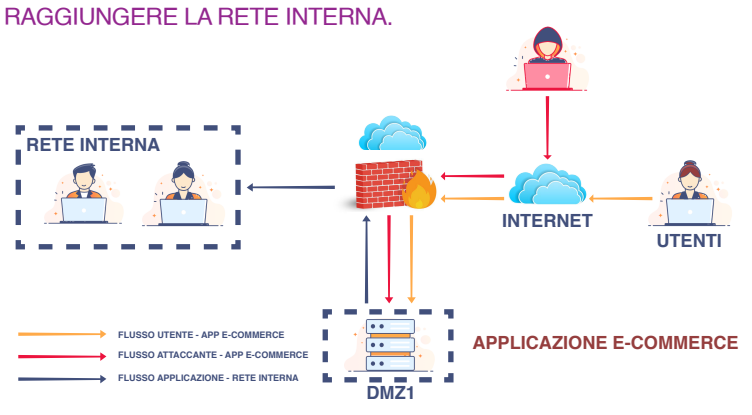
TRACCIA FINALE W20D4

CON RIFERIMENTO ALLA FIGURA RISPONDERE AI SEGUENTI QUESITI

TRACCIA:

ARCHITETTURA DI RETE:

L'APPLICAZIONE DI E-COMMERCE DEVE ESSERE DISPONIBILE PER GLI UTENTI TRAMITE INTERNET PER EFFETTUARE ACQUISTI SULLA PIATTAFORMA.
LA RETE INTERNA È RAGGIUNGIBILE DALLA DMZ PER VIA DELLE POLICY SUL FIREWALL, QUINDI SE IL SERVER IN DMZ VIENE COMPROMESSO POTENZIALMENTE UN ATTACCANTE POTREBBE RAGGIUNGERE LA RETE INTERNA.



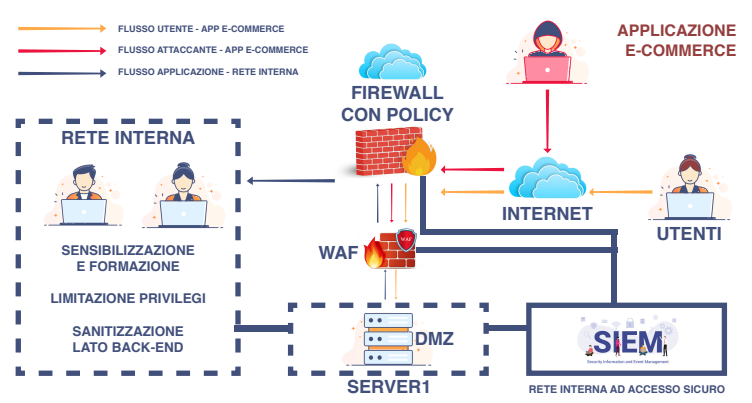
1. AZIONI PREVENTIVE:

QUALI AZIONI PREVENTIVE SI POTREBBERO IMPLEMENTARE PER DIFENDERE L'APPLICAZIONE WEB DA **ATTACCHI DI TIPO SQLI OPPURE XSS** DA PARTE DI UN UTENTE MALINTENZIONATO?

MODIFICATE LA FIGURA IN MODO DA EVIDENZIARE LE IMPLEMENTAZIONI

COME AZIONI PREVENTIVE IN CASO DI UNA MINACCIA DEL GENERE SQLI E XSS DA PARTE DI UN UNTENTE MALINTENZIONATO, CHE RICORDIAMO POTER ESSERE SIA ALL'INTERNO CHE ALL'ESTERNO DELL'ATTIVITÀ DI E-COMMERCE IN QUESTIONE, IO PROPORREI UNA SERIE DI OPZIONI CHE ELENCO DI SEGUITO:

- WEB APPLICATION FIREWALL (WAF): UN DISPOSITIVO DI SICUREZZA DEDICATO NELLO SPECIFICO A PROTEGGERE APPLICAZIONI DA ATTACCHI QUALI SQL INJECTION E XROSS SITE SCRIPTING.
- VALIDAZIONE E SANITIZZAZIONE DEGLI INPUT: BISOGNA ASSICURARSI CHE TUTTI GLI INPUT FORNITI DAGLI UTENTI SIANO VALIDATI SIA SUL LATO CLIENT CHE SUL LATO SERVER, ACCETTANDO SOLO INPUT CHE SODDISFANO DETERMINATI CRITERI. INOLTRE ÈNECESSARIO RIMUOVERE O CODIFICARE CARATTERI SPECIALI CHE POSSONO ESSERE UTILIZZATI IN ATTACCHI SOLI O XSS.
- HTTPS: UTILIZZARE HTTPS PER CRITTOGRAFARE IL TRAFFICO TRA IL CLIENT E IL SERVER, È UTILE A PROTEGGERE I DATI IN TRANSITO.
- AGGIORNAMENTI E PATCH: MANTENENDO L'APPLICAZIONE E IL SUO ENVIRONMENT (SERVER, DATABASE, FRAMEWORK, ECC.) AGGIORNATI CON LE ULTIME PATCH DI SICUREZZA, SI POSSONO PREVENIRE ATTACCHI CHE SFRUTTANO BUG NOTI O VULNERABILITÀ CHE NE DERIVANO.
- SENSIBILIZZAZIONE E FORMAZIONE: È MOLTO IMPORTANTE FORMARE GLI SVILUPPATORI/PERSONALE INTERNO CHE HA ACCESSO AI VARI END-POINT ALLE BEST PRACTICE DI PROGRAMMAZIONE SICURA E AI RISCHI DI SICUREZZA COMUNI E NOTI COME SQLI E XSS.
- LIMITAZIONE DEI PRIVILEGI: LE CONNESSIONI AL DATABASE DOVREBBERO USARE ACCOUNT CON IL MINIMO LIVELLO DI PRIVILEGI NECESSARIO PER SVOLGERE IL LAVORO.
- LOGGING E MONITORAGGIO: POTREBBE ESSERE UTILE MANTENERE LOG DETTAGLIATI DELLE ATTIVITÀ PER UNA VISIONE CENTRALIZZATA DELLA SICUREZZA, MAGARI CON DEI SISTEMI SIEM, E MONITORARE LE APP E I SISTEMI PER INDIVIDUARE E REAGIRE RAPIDAMENTE A QUALSIASI ATTIVITÀ SOSPETTA ED EVENTUALI MINACCE O ATTACCHI IN CORSO.
- VULNERABILITY ASSESSMENT: FARE CONTINUE CAMPAGNE E TESTARE PERIODICAMENTE L'APPLICAZIONE FACENDO DEI PENETRATION TEST È UN METODO UTILE A SCOPRIRE EVENTUALI FALLE E PORVI RIMEDIO PRIMA CHE POSSANO VENIRE SFRUTTATE DA MALINTENZIONATI
- DIFFERENTIAL BACKUP: SERVE ESEGUIRE BACKUP REGOLARI DEI DATI E DEL CODICE DELL'APPLICAZIONE SU SISTEMI DI STORAGE SICURI E TESTARE REGOLARMENTE LA PROCEDURA DI RIPRISTINO. IL DIFFERENTIAL BACKUP È UNA SOLUZIONE MENO DISPENDIOSA A LIVELLO DI TEMPO IN QUANTO PERMETTE DI IMPLEMENTARE SOLO DATI CHE SONO STATI MODIFICATI DALL'ULTIMO FULL BACKUP CHE VENGONO COPIATI E SALVATI.
- SISTEMI DI RILEVAMENTO E PREVENZIONE DELLE INTRUSIONI (IDS/IPS): SI POSSONO IMLEMENTARE IDS/IPS PER RILEVARE COMPORTAMENTI ANOMALI O SCHEMI DI ATTACCO E PRENDERE AZIONI AUTOMATICHE PER PREVENIRE O MITIGARE GLI ATTACCHI.

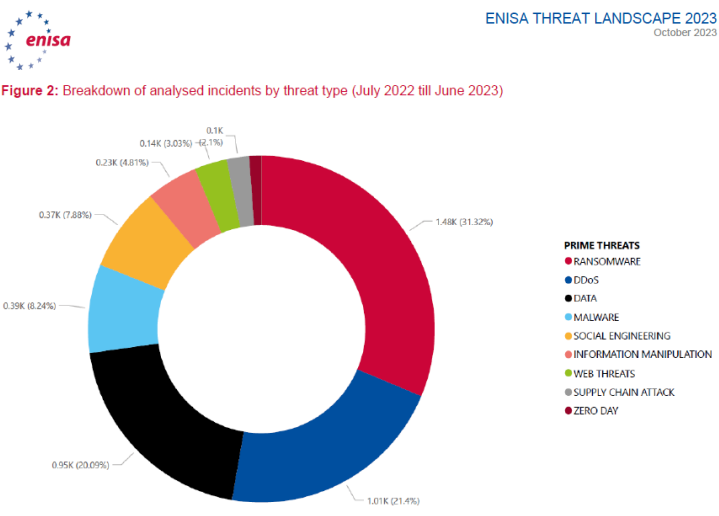


2. IMPATTI SUL BUSINESS:

L'APPLICAZIONE WEB SUBISCE **UN ATTACCO DI TIPO DDOS DALL'ESTERNO** CHE RENDE L'APPLICAZIONE NON RAGGIUNGIBILE PER 10 MINUTI. CALCOLARE L'IMPATTO SUL BUSINESS DOVUTO ALLA NON RAGGIUNGIBILITÀ DEL SERVIZIO, CONSIDERANDO CHE IN MEDIA OGNI MINUTO GLI UTENTI SPENDONO 1.500 € SULLA PIATTAFORMA DI E-COMMERCE **(15.000 € IN TOT.)**.

FARE EVENTUALI VALUTAZIONI DI AZIONI PREVENTIVE CHE SI POSSONO APPLICARE IN QUESTA PROBLEMATICA (ACCETTAZIONE DEL RISCHIO O RIDUZIONE).

DICIAMO CHE, SENZA AVERE UNA SITUAZIONE PRECISA RIGUARDO IL SETTORE DELL'ATTIVITÀ E LA CATEGORIA MERCEOLOGICA, LA SUA COLLOCAZIONE E LA SITUAZIONE GEOPOLITICA, NONCHÈ ALTRI FATTORI CHE AD OGGI NON SAREI IN GRADO DI VALUTARE, MI LIMITEREI ALLA CONSIDERAIZONE CHE, TRATTANDOSI DI UNA PERDITA DI 15.000 EURO IN DIECI MINUTI, SI TRATTI DI UN'ATTIVITÀ DI MEDIA ENTITÀ CON UN BUDGET NON ELEVATISSIMO DA INVESTIRE IN SECURITY OPERATIONS E BCP, MA CHE PUò COMUNQUE TROVARE SOLUZIONI OTTIMALI PER PROTEGGERE IL SISTEMA DA UN ATTACCO DI TIPO DDOS.
UN'ACCETTAZIONE DEL RISCHIO POTREBBE NON ESSERE UNA BUONA OPZIONE TRATTANDOSI DI HOSTING CHE DEVE RENDERE DISPONIBILE IL PROPRIO SERVIZIO ALLA CLIENTELA E RISPETTARE LA TRIADE CIA. VEDIAMO QUINDI QUALI AZIONI PREVENTIVE SI POTREBBERO IMPLEMENTARE, DATO CHE UN ATTACCO DDOS, COME POSSIAMO VEDERE DAI REPORT DI ENISA AGGIORNATI A GIUGNO DEL 2023, È SECONDO IN FREQUENZA SOLO AI RANSOMWARE.



GLI ATTACCHI DDOS SONO DIVENTATI PIÙ COMPLESSI, SPOSTANDOSI VERSO RETI MOBILI E DISPOSITIVI INTERNET OF THINGS (IOT) ORA UTILIZZATI NELLA CYBERWARFARE. SECONDO IL REPORT IMPERVA GLOBAL DDOS THREAT LANDSCAPE DEL 2023 RIPORTA UN INCREMENTO DELL'82% DEGLI ATTACCHI DDOS A LIVELLO DI APPLICAZIONE NEL 2022 RISPETTO AL 2021, CON ATTACCHI AL SETTORE DEI SERVIZI FINANZIARI CRESCIUTI DEL 121% ANNO SU ANNO.
IN ITALIA, C'È STATA UNA NOTEVOLE CRESCITA DEGLI ATTACCHI DDOS NEL PRIMO SEMESTRE DEL 2023. RISPETTO AL 2022, QUANDO GLI ATTACCHI DDOS RAPPRESENTAVANO IL 4% DEL TOTALE, NEL 2023 LA PERCENTUALE È SALITA AL 30%, UNA CRESCITA NOTEVOLE E MOLTO PIÙ ALTA DELLA MEDIA GLOBALE CHE SI ATTESTA AL 7,9%. CIÒ INDICA CHE QUASI UN TERZO DEGLI ATTACCHI RILEVATI IN ITALIA SONO DI TIPO DDOS, UNA QUOTA CHE RIFLETTE CIRCA IL 37% DEL TOTALE DEGLI ATTACCHI DDOS REGISTRATI A LIVELLO MONDIALE. QUESTO AUMENTO È STATO COLLEGATO ALL'ATTIVISMO E ALLA GUERRA INFORMATIVA, CHE MIRANO A INTERROMPERE LE OPERAZIONI DI UN'ENTITÀ PER ATTIRARE L'ATTENZIONE MEDIATICA SU CAUSE POLITICHE O SOCIALI. SI TRATTA DI UN FENOMENO CHE HA VISTO L'ITALIA DIVENTARE UN TEATRO SIGNIFICATIVO PER TALI ATTIVITÀ HACKTIVISTE.
È DUNQUE ABBASTANZA CERTO CHE DA UNA MINACCIA DEL GENERE BISOGNA DIFENDERSI IMPLEMENTANDO CIÒ CHE È NECESSARIO PER RIDURRE IL RISCHIO, ANCHE A COSTO DI ANDARE OLTRE LA CIFRA DEI 15 MILA EURO PERSI IN DIECI MINUTI.

- UNA DELLE SOLUZIONI PIÙ FACILI SAREBBE CAMBIARE IL DNS, CHE ANDREBBE A SUPPLEMENTO CONTRIBUENDO A DISTRIBUIRE IL CARICO DI TRAFFICO TRA PIÙ SERVER (LOAD BALANCING), INCREMENTANDO LA RESILIENZA DELL'ARCHITETTURA IT CONTRO GLI ATTACCHI, INTOLTRE L'USO DI SERVIZI DI DNS SECONDARIO (O DI FAILOVER) PUÒ GARANTIRE CHE IL TUO DOMINIO RIMANGA ONLINE ANCHE SE IL PROVIDER DNS PRIMARIO SUBISCE UN'INTERRUZIONE.
- È POSSIBILE PREVENIRE GLI ATTACCHI DDOS MEDIANTE STRUMENTI DI MONITORAGGIO DEL TRAFFICO IN TEMPO REALE CHE RILEVANO E PREVENGONO I PICCHI DI TRAFFICO ANOMALI, FORNENDO LA POSSIBILITÀ DI REAGIRE PRONTAMENTE PRIMA CHE L'ATTACCO CAUSI DANNI MAGGIORI.
- L'INTRODUZIONE DI UN SERVIZIO COME CLOUDFLARE PER MITIGARE GLI ATTACCHI DDOS: OFFRE DIVERSI SERVIZI PROGETTATI PER PROTEGGERE QUALSIASI COSA CONNESSA A INTERNET DAGLI ATTACCHI DDOS E FORNISCE PROTEZIONE ILLIMITATA CONTRO GLI ATTACCHI DDOS PER I SITI WEB (HTTP/HTTPS), CHE È INCLUSA GRATUITAMENTE IN TUTTI I PIANI DI SERVIZIO DELLE APPLICAZIONI WEB DI CLOUDFLARE. INOLTRE, CLOUDFLARE HA UNA CAPACITÀ DI RETE CONSIDEREVOLE E PUÒ MITIGARE LA MAGGIOR PARTE DEGLI ATTACCHI IN MENO DI 3 SECONDI, IL CHE È UTILE DATO CHE IL TEMPO DI RISPOSTA RAPIDO È CRUCIALE DURANTE UN ATTACCO DDOS.
- LOGGING E MONITORAGGIO: POTREBBE ESSERE UTILE MANTENERE LOG DETTAGLIATI DELLE ATTIVITÀ PER UNA VISIONE CENTRALIZZATA DELLA SICUREZZA, MAGARI CON DEI SISTEMI SIEM, E MONITORARE LE APP E I SISTEMI PER INDIVIDUARE E REAGIRE RAPIDAMENTE A QUALSIASI ATTIVITÀ SOSPETTA ED EVENTUALI MINACCE O ATTACCHI IN CORSO.
- È MOLTO UTILE ANCHE INSERIRE DELLE PIATTAFORME DI THREAT INTELLIGENCE
- È IMPORTANTE VALUTARE ANCHE DANNI CHE RIGUARDANO LA REPUTAZIONE DELLA NOSTRA ATTIVITÀ E GLI ACCORDI COMMERCIALI CHE ABBIAMO CON ALTRE AZIENDE. PER QUESTO TUTTE LE ALTRE CONTROMISURE SONO UTILI AL FINE DI LIMITARE I RISCHI E NON PERMETTERE AD EVENTUALI MINACCE ESTERNE DI TENERE GIÙ I SISTEMI A LUNGO, CERCANDO DI MINIMIZZARE LE TEMPISTICHE DI RIPRISTINO E L'INTEGRITÀ DEL DATABASE E DATI SENSIBILI.

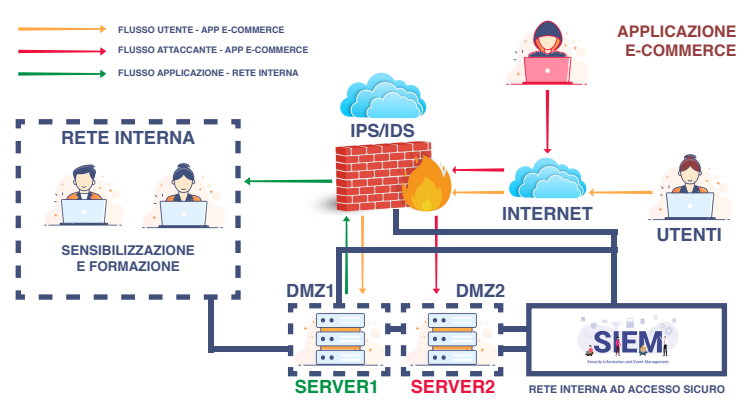
3. RESPONSE:

L'APPLICAZIONE WEB VIENE INFETTATA DA UN MALWARE. LA VOSTRA PRIORITÀ È CHE IL MALWARE NON SI PROPAGHI SULLA VOSTRE RETE, MENTRE NON SIETE INTERESSATI A RIMUOVERE L'ACCESSO DA PARTE DELL'ATTACCANTE ALLA MACCHINA INFETTATA.

MODIFICATE LA FIGURA IN SLIDE 2 CON LA SOLUZIONE PROPOSTA.

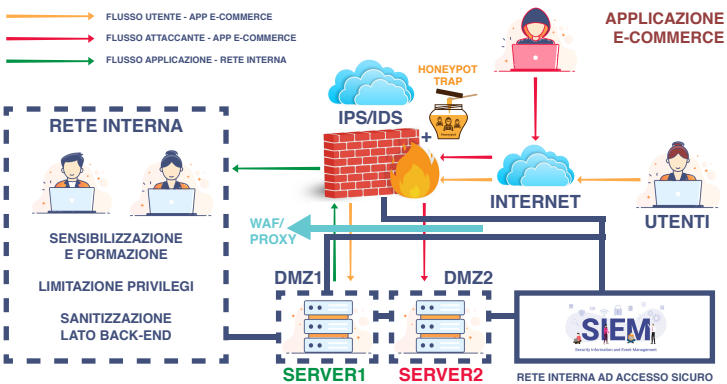
IN QUESTO CASO, ESSENDO GIÀ L'APPLICAZIONE STATA INFETTATA DAL MALWARE, AVENDO PREVENTIVAMENTE PROVVEDUTO AD UNA SEGMENTAZIONE DI RETE (ASSEGNANDO DIVERSI LIVELLI DI SICUREZZA ALLE DIVERSE AREE DELLA RETE, COME AD ESEMPIO DMZ, OVVERO L'AREA DELLA RETE CHE ESPONE I SERVIZI ACCESSIBILI DA INTERNET), LA COSA PIÙ UTILE DA FARE È ISOLARE IL SERVER1 INFETTO DALLA RETE E METTERLO IN "RETE DI QUARANTENA". LA SEGMENTAZIONE INCLUDE TUTTE QUELLE ATTIVITÀ CHE PERMETTONO DI DIVIDERE UNA RETE IN DIVERSE LAN O VLAN, IN MODO TALE CHE IN CASO DI NECESSITÀ SI POSSA SEPARARE IL SISTEMA INFETTO DAGLI ALTRI COMPUTER SULLA RETE, CREANDO UNA RETE AD HOC. CON LE DOVUTE CONFIGURAZIONI A LIVELLO NETWORK CREANDO UN SISTEMA DI CONTENIMENTO, IL MALWARE RISULTEREBBE COSÌ SEPARATO DAL RESTO DELLA RETE ED INCAPACE DI RIPRODURSI E DIFFONDERSI, MA SE NE PUÒ STUDIARE ED ANALIZZARE IL COMPORTAMENTO IN UN SECONDO MOMENTO SENZA CHE SI PROPAGHI SULLA RETE INTERNA. NEL FRATTEMPO SI SWITCHA SUL SERVER2, CHE AVRÀ TUTTI I SUOI BACKUP, E CHE POTRÀ CONTINUARE AD EROGARE IL SERVIZIO GARANTENDO LA CONTINUITÀ OPERATIVA DELL'HOSTING.
IN QUESTO CASO UN IPS/IDS SAREBBE ANCORA PIÙ CONSIGLIABILE, QUINDI SI PROCEDE A VERIFICARE SE IL DISPOSITIVO CHE FA DA FIREWALL NE SUPPORTA L'IMPLEMENTAZIONE.
INOLTRE UN SIEM ANCHE IN QUESTO CASO SAREBBE CONSIGLIABILE; INSERENDO UN SISTEMA DI THREAT INTELLIGENCE CHE ABBIA SONDE SIA SUI SERVER CHE A LIVELLO DI RETE ED ANCHE A LIVELLO DI END-POINT SI POTRANNO RILEVARE COMPORTAMENTI ANOMALI O SCHEMI DI ATTACCO E PRENDERE AZIONI AUTOMATICHE PER PREVENIRE O MITIGARE GLI ATTACCHI.
ALTRE AZIONI PREVENTIVE UTILI SONO:

- RIDONDANZA DEI SERVER E DEI NETWORK: PER UNA MAGGIORE RESILIENZA E TOLLERANZA AGLI ERRORI DELL'APPLICAZIONE WEB, BISOGNA ASSICURARSI CHE CI SIA PIÙ DI UN SERVER AD OSPITARLA, IN CASO DI FALLIMENTO DI UNO DEI SERVER POSSONO SEMPRE CONTINUARE AD EROGARE IL SERVIZIO GLI ALTRI PRESENTI (FAILOVER CLUSTER), INOLTRE AIUTEREBBE IL BILANCIAMENTO DEL CARICO. PER QUANTO RIGUARDA IL NETWORK È BUONA PRASSI CHE LA RETE SIA PROGETTATA CON PERCORSI RIDONDANTI PER EVITARE SINGLE POINT OF FAILURE CHE POTREBBE RENDERE L'APPLICAZIONE INACCESSIBILE. POSSIAMO IMPLEMENTARE UN RAID CON UNO O PIÙ DISCHI PER GARANTIRE AL CONTINUITÀ DI SERVIZIO HOSTING. COME SOLUZIONE MENO COSTOSA C'È IL RAID-1, OPPURE UN RAID-5 CHE AVREBBE PIÙ PRESTAZIONE IN LETTURA, MA NON GARANTISCE LA PROTEZIONE DEI DATI.
- DIFFERENTIAL BACKUP: SERVE ESEGUIRE BACKUP REGOLARI DEI DATI E DEL CODICE DELL'APPLICAZIONE SU SISTEMI DI STORAGE SICURI E TESTARE REGOLARMENTE LA PROCEDURA DI RIPRISTINO. IL DIFFERENTIAL BACKUP È UNA SOLUZIONE MENO DISPENDIOSA A LIVELLO DI TEMPO IN QUANTO PERMETTE DI IMPLEMENTARE SOLO DATI CHE SONO STATI MODIFICATI DALL'ULTIMO FULL BACKUP CHE VENGONO COPIATI E SALVATI. CIASCUNA COMPONENTE SULLA QUALE VIENE ESEGUITO UN BACKUP PER BUONA PRASSI DEVE ESSERE STACCATA DAL SISTEMA A FINE BACKUP E NON FAR PARTE DI ALCUNA RETE.
- UN HONEYPOT PUÒ ESSERE IMPIEGATO COME PARTE DELLA STRATEGIA DI SICUREZZA: È UNA RISORSA DI SISTEMA CHE SEMBRA ESSERE PARTE DELLA RETE MA È IN REALTÀ ISOLATA E MONITORATA. LA SUA FUNZIONE È DI ATTIRARE GLI ATTACCANTI, CHE, PENSANDO DI ACCEDERE A PARTI SENSIBILI DELLA RETE, SI RIVELERANNO E VERRANNO INTRAPPOLATI. L'HONEYPOT PUÒ AIUTARE A DISTOGLIERE GLI ATTACCANTI DALLE RISORSE REALI E FORNIRE INTELLIGENZA SULLE TECNICHE E GLI STRUMENTI UTILIZZATI DAGLI ATTACCANTI. PER IMPLEMENTARE UN HONEYPOT, DOVRESTI POSIZIONARLO IN UNA ZONA DELLA RETE BEN MONITORATA MA CHE SEMBRI ATTRAENTE PER UN ATTACCANTE. AD ESEMPIO, POTREBBE ESSERE POSTO NELLA DMZ O IN UNA SUBNET CHE APPARE COME SE AVESSE ACCESSO A DATI SENSIBILI, MA CHE IN REALTÀ È ISOLATA DAL RESTO DELLA RETE. CI SONO DIVERSI TIPI DI HONEYPOT, DA QUELLI DI BASSA INTERAZIONE, CHE SIMULANO SOLO ALCUNI SERVIZI O APPLICAZIONI, A QUELLI DI ALTA INTERAZIONE, CHE SONO SISTEMI COMPLESSI E POSSONO INTERAGIRE CON L'ATTACCANTE IN MODO PIÙ PROFONDO.
- CONFIGURARE UN PROXY: ESSENDO UN SERVER CHE FUNGE DA INTERMEDIARIO PER LE RICHIESTE DA PARTE DI CLIENT IN CERCA DI RISORSE DA ALTRI SERVER, IL TRAFFICO INTERNET VIENE REINDIRIZZATO ATTRAVERSO QUESTO SERVER. NEL CONTESTO DELLA SICUREZZA, I PROXY POSSONO ESSERE USATI PER FILTRARE CONTENUTI, NASCONDERE L'INDIRIZZO IP EFFETTIVO DI UN UTENTE E PROTEGGERE LA RETE INTERNA DA ACCESSI DIRETTI. SI POTREBBE CONFIGURARE UN PROXY COME UN GATEWAY CHE DEVONO ATTRAVERSARE TUTTI I DATI , PERMETTENDOTI DI ANALIZZARE E FILTRARE IL TRAFFICO SOSPETTO.
- DATA CENTER GEOGRAFICAMENTE DISTRIBUITI: COME SOLUZIONE PIÙ COSTOSA IN CASO DI PRESENZA DI FONDI E IN BASE ALLA CATEGORIA MERCEOLOGICA DELL'ATTIVITÀ E IL SUO ANDAMENTO, SI PUÒ VALUTARE DI DISTRIBUIRE L'INFRASTRUTTURA SU PIÙ DATA CENTER IN DIVERSE AREE GEOGRAFICHE PER PROTEGGERLA DA DISASTRI NATURALI O GUASTI DI RETE LOCALIZZATI.
- SOFTWARE STILE DARKTRACE: SI TRATTA DI SOLUZIONI CHE USANO L'INTELLIGENZA ARTIFICIALE E IL MACHINE LEARNING PER RILEVARE E RISPONDERE A MINACCE IN TEMPO REALE NELLA RETE. QUESTI SISTEMI SI BASANO SULL'ANALISI COMPORTAMENTALE E POSSONO IDENTIFICARE ATTIVITÀ SOSPETTE O ANOMALE CHE POTREBBERO INDICARE LA PRESENZA DI MALWARE O ALTRI TIPI DI ATTACCHI. SI INTEGRANO NELLA RETE E ANALIZZANO COSTANTEMENTE IL TRAFFICO ALLA RICERCA DI MODELLI INSOLITI, SPESSO LAVORANDO IN COMBO CON ALTRI DISPOSITIVI DI SICUREZZA COME I FIREWALL.



4. SOLUZIONE COMPLETA:

UNIRE I DISEGNI DELL'AZIONE PREVENTIVA E DELLA RESPONSE (UNIRE SOLUZIONE 1 E 3)



5. MODIFICA «PIÙ AGGRESSIVA» DELL'INFRASTRUTTURA

(SE NECESSARIO/FACOLTATIVO MAGARI INTEGRANDO LA SOLUZIONE AL PUNTO 2)

IN CASO NON BASTASSE L'ISOLAMENTO E IL RESTO DELLE AZIONI INDICATE NEL PUNTO 2, TRA LE MODIFICHE PIÙ AGGRESSIVE PUÒ RIENTRARE LA RIMOZIONE DEL SISTEMA INFETTO. QUANDO DIVENTA NECESSARIO RIMUOVERE OGNI TRACCIA DELL'INCIDENTE BISOGNA SMALTIRE O RECUPERARE I DISCHI DI STORAGE SU CUI SI TROVA IL SISTEMA ATTACCATO. ESISTONO DIVERSI METODI TRA I QUALI ABBIAMO VISTO IL PURGE (RIMOZIONE DEI DATI CON METODI FISICI, COME L'UTILIZZO DEI MAGNETI) IL DESTROY (DISTRUZIONE TOTALE DEL DISCO MEDIANTE ALTE TEMPERATURE, O DISINTEGRAZIONE, ECC) E IL CLEAR (RIMOZIONE DEI DATI CON TECNICHE DI FACTORY RESET O SOVRASCIVENDO IL DISCO MOLTE VOLTE). OVVIAMENTE PER NON COMPROMETTERE DEL TUTTO L'ATTIVITÀ SI PRESUME CHE CI SIANO TUTTI I SISTEMI DI BACKUP NECESSARI E ALTRI SERVER/SEDI.

SI PUÒ RICORRERE AL DRAAS (DISASTER RECOVERY AS A SERVICE): I CLOUD PROVIDER METTONO A DISPOSIZIONE DELLE COMPAGNIE UN'INFRASTRUTTURA IN CLOUD CHE VIENE IMMEDIATAMENTE ATTIVATA IN CASO DI DISASTRO SUL SITO PRIMARIO DELLA COMPAGNIA. TRA GLI SVANTAGGI CI SONO I TEMPI DI LATENZA DELLO "SWITCH" DAL SITO PRIMARIO AL SECONDARIO. TUTTAVIA È CONVENIENTE IN QUANTO SI PAGA IL SERVIZIO QUANDO VI SI ATTINGE SOLO IN CASO DI NECESSITÀ. IN QUESTO CASO SI TRATTEREBBE DI SPOSTAMENTO DEL RISCHIO.