inthecyber

intelligence & defense advisors

Smart Working Security Control

inthecyber

intelligence & defense advisors

InTheCyber Group SA

Via Vegezzi, 4 - 6900 Lugano, CH - T. +41 91 911 7 301

InTheCyber s.r.l.

Piazza Ernesto De Angeli, 3 - 20146 Milano, IT - T. +39 02 4801 3067

Vista la difficile situazione che moltissime aziende si trovano ad affrontare in questi giorni, attenendosi a quanto emanato dai Governi, si stanno muovendo per attivare piattaforme che agevolino i propri dipendenti nel lavorare da casa grazie alla metodologia del lavoro agile o smart working.
Alla luce di un aumento esponenziale degli accessi alle reti aziendali per mezzo di reti domestiche “untrusted” o non sicure, aumentano di pari passo i rischi a cui le risorse delle reti aziendali sono esposte, permettendo così ai cyber criminali di penetrare all'interno della rete attraverso il riutilizzo di credenziali disponibili sul deep web, tramite mail di phishing e spoofing o semplicemente attraverso perimetri resi deboli da possibili misconfigurazioni o da un'inappropriata postura di sicurezza, avendo così accesso a dati e informazioni sensibili in tempi quasi istatanei.

InTheCyber, azienda leader nel settore da oltre dieci anni, mette a disposizione delle PA e PM **Smart Working Security Control**, un pacchetto di servizi studiati ad hoc per proteggere tutti i lavoratori, le aziende e tutti gli operatori delle PA in questo particolare momento storico.

OVERVIEW DELL'OFFERTA

SECURITY POSTURE ANALYSIS

Il servizio prevede la verifica delle configurazioni dei mail server e del livello di password utilizzate, in modo da indicare le contromisure da attuare per evitare gli attacchi più comuni e più probabili di cui potrebbero essere vittime via email.

ACTIVE DIRECTORY POSTURE ANALYSIS

Il servizio permette di individuare tutte le misconfigurazioni e l'incorretta assegnazione di permessi all'interno dell'ambiente Active Directory, fornendo una misurazione del rischio a cui l'azienda è esposta e consigliando le contromisure da adottare

IT INFRASTRUCTURE ANALYSIS

Il servizio prevede l'analisi delle configurazioni delle piattaforme/device coinvolti nel processo di Smart Working al fine di evidenziare le criticità dal punto di vista della sicurezza ed indicando le contromisure necessarie.

MANAGED DETECTION & RESPONSE

Il servizio prevede l'installazione di agent intelligenti (se non già presenti) sui device utilizzati dai collaboratori in Smart Working ed il loro monitoraggio da parte del Cyber Center di *InTheCyber* per la rilevazione sul nascere di potenziali minacce e la loro rapida neutralizzazione.

Tutti i servizi sono stati pensati ed ideati per poter essere effettuati da remoto

SECURITY POSTURE ANALYSIS

1

Awareness

Per una difesa ottimale serve innanzitutto capire cosa va difeso, dove inizia e quali sono i punti di accesso da tenere sotto controllo. Una delle entrate più utilizzate dagli attaccanti, per facilità e buona riuscita, è la posta elettronica, i cyber criminali, infatti, sfruttando le errate configurazioni del server, spesso inviano email camuffando l'inidirizzo del mittente in modo che sembri spedita dal CEO dell'azienda, da un fornitore che chiede di saldare una fattura su un nuovo conto corrente, o ancora da un legale che chiede l'invio di documeti riservati.

2

Password

Oltre al problema della configurazione errata dei server aziendali di posta, un altro problema che causa spesso intrusioni informatiche all'interno delle aziende è il riutilizzo delle password da parte dei dipendenti.
Molto spesso, quando ad essere attaccate sono aziende che offrono servizi pubblici sul web (vedi social, mail, log-in ecc...), vengono rubate le liste con le credenziali di tutti gli utenti registrati, successivamente vendute e acquistate sul mercato nero digitale.

3

Security Posture Analysis

Il servizio di Security Posture Analysis permette al cliente di divenire consapevole della propria superficie di attacco e di attuare contromisure a costo zero per evitare gli attacchi più comuni e probabili di cui potrebbe essere vittima.

4

Il Servizio

Il servizio viene erogato nei seguenti modi:

1) Controllo della configurazione del server di posta da remoto verificando la possibilità di inviare mail spoofate sia a soggetti interni che esterni all'azienda.
2) Controllo della presenza di credenziali nei database di password rubate.
3) Mappatura dei servizi esposti su internet dall'azienda.

5

Il Report

I risultati delle analisi vengono consegnati tramite la stesura di un report che comprende due parti:

1) Executive summary: riepilogo ad alto livello della situazione della sicurezza istanziata ai test effettuati.
2) Technical report: documento indirizzato al personale tecnico che evidenzia le contromisure proposte.

inthecyber
intelligence & defense advisors

InTheCyber Group SA
Via Vegezzi, 4 - 6900 Lugano, CH - T. +41 91 911 7 301

InTheCyber s.r.l.
Piazza Ernesto De Angeli, 3 - 20146 Milano, IT - T. +39 02 4801 3067

ACTIVE DIRECTORY SECURITY POSTURE ANALYSIS

1

Active Directory

Active directory è un servizio di rete offerto dai server Windows che integra il database con altre funzionalità che consentono di gestire in maniera centralizzata un dominio e tutte le relative risorse, gli utenti e i servizi.

La pervasività di questo servizio fa si che diventi anche molto delicato in termini di sicurezza, in quanto una sua cattiva configurazione rende vulnerabile l'intera infrastruttura di rete aziendale e può consentire ad un hacker di penetrare con facilità all'interno del perimetro di sicurezza.

2

Database

Il database di Active Directory è strutturato in maniera gerarchica, con contenitori all'interno dei quali sono raggruppati i vari elementi che fungono da unità organizzative.

E' evidente come Active Directory diventi un elemento essenziale per la gestione e il mantenimento della sicurezza delle infrastrutture di rete di un'azienda, ma solo se è stata configurata correttamente in precedenza. Se ciò non è avvenuto, rischia di trasformarsi in un'arma a doppio taglio e di offrire a potenziali attaccanti pericolosi punti di accesso alla rete. Ciò rappresenterebbe una concreta minaccia per la disponibilità, integrità e riservatezza delle risorse.

3

Security Posture Analysis

Il servizio di Security Posture Analysis permette di individuare tutte le misconfigurazioni e la scorretta assegnazione dei permessi all'interno dell'ambiente Active Directory, fornendo una misurazione del rischio a cui l'azienda è esposta e consigliando le contromisure da adottare.

In mancanza delle dovute restrizioni, i criminali hacker potrebbero avere accesso alla totalità della rete, e, senza destare sospetti, mettere in atto operazioni di sabotaggio, spionaggio o furto di dati.

4

Il Servizio

Ill servizio viene erogato tramite un accesso in VPN alla rete del cliente o in loco.

L'ambiente Active Directory verrà ispezionato, a titolo di esempio, per le seguenti problematiche:

- Anomalie
- Oggetti inutilizzati e obsoleti
- Account Privilegiati
- TRUST

5

Il Report

I risultati delle analisi vengono consegnati tramite la stesura di un report così strutturato:

1) Executive summary: riepilogo ad alto livello della situazione della sicurezza istanziata ai test effettuati.
2) Technical report: documento indirizzato al personale tecnico qualificato che sia in grado di capire le problematiche evidenziate e di apportare le contromisure consigliate che accompagnano la descrizione delle problematiche.

inthecyber
intelligence & defense advisors

InTheCyber Group SA
Via Vegezzi, 4 - 6900 Lugano, CH - T. +41 91 911 7 301

InTheCyber s.r.l.
Piazza Ernesto De Angeli, 3 - 20146 Milano, IT - T. +39 02 4801 3067

IT INFRASTRUCTURE ANALYSIS

Contesto

Basandosi sul paradigma proprietario G.A.T.E. (Gather, Analyze, Test, Enhance), gli esperti *ITC* analizzeranno con un approccio white box le configurazioni di specifiche piattaforme, device, e ambienti software coinvolti in flussi di informazioni critiche.
Una volta raccolte le configurazioni si passerà all'analisi dettagliata di ogni ambiente, eventualmente effettuando delle simulazioni preventive in laboratorio, e stilando quindi una lista di punti vulnerabili o carenti, su cui risulti necessario operare delle migliorie. Verrà verificato il massimo livello di sicurezza ottenibile dal tuning dei dispositivi oggetto di analisi, proponendo di volta in volta la migliore configurazione possibile ed evidenziando eventuali limiti intrinsechi del dispositivo analizzato.

Aree di intervento

Network appliances: raccolta di configurazioni degli apparati di rete a livello 1, 2,3 dello stock di riferimento ISO/OSI, cioè dispositivi come router, load balancer, switch e hub.
Security appliances: raccolta configurazioni degli apparati di difesa, cioè firewall, proxy, IDS/IPS, ecc...
Active directory infrastructure: raccolta di configurazioni domain controllers e dei sistemiad esso connessi in ambito Acive Directory.
End Points: raccolta delle impostazioni e configurazioni dei sistemi situati agli estremi della catena, come le workstations e i server, con le loro applicazioni installate.

In tutte e quattro le aree di intervento esposte al punto 2 le configurazioni verranno analizzate nel dettaglio dal nostro team per evidenziarne le criticità da un punto di vista della sicurezza, indicando puntualmente le modifiche da attuare per portare ai massimi livelli (limitatamente alle capacità intrinseche dei dispositivi in uso) la protezione aziendale.

Le Fasi

1) Gather: Il Cliente fornisce ogni dettaglio dulla rete da analizzare, i device coinvolti, le configurazioni e le informazioni ambientali e di deployment.
2) Analyze: una volta acquisito il dataset, *InTheCyber* analizza i rischi e le vulnerabilità, evidenziando eventuali misconfigurazioni.
3) Test: Il principio di difesa approfondita è applicato per ogni device coinvolto, per definire un sistema di difesa multi-layer.
4) Enhance: Le raccomandazioni di sicurezza vengono valutate ed implementate dal cliente, in preparazione per le successive iterazioni del ciclo.

Il Report

Il deliverable di questa attività sarà un report indicante ogni misconfigurazione rilevata, associata ad una relativa strategia di rimedio. Verranno specificate puntualmente le modifiche da effettuare a livello infrastrutturale, di policy e sulle configurazioni dei dispositivi.
Verranno inoltre evidenziati eventuali limiti intrinsechi dei dispositivi e/o ambienti analizzati che non permettano di raggiungere lo standard di sicurezza desiderato.

inthecyber
intelligence & defense advisors

InTheCyber Group SA
Via Vegezzi, 4 - 6900 Lugano, CH - T. +41 91 911 7 301

InTheCyber s.r.l.
Piazza Ernesto De Angeli, 3 - 20146 Milano, IT - T. +39 02 4801 3067

MANAGED DETECTION & RESPONSE

Il Contesto

il CyberSecurity Center di *InTheCyber* interviene anche nei casi in cui l'errore umano rischia di compromettere la sicurezza dell'intera rete, e innalza il livello di monitoraggio riuscendo a individuare anche le minacce che i più comuni strumenti di detection automatici non segnalano.

Il servizio di Managed Detection and Response garantisce le professionalità dei Cyber Threat Analysts di *ITC* al servizio di monitoraggio delle workstation dei dipendenti in Smart Woking, grazie all'installazione di un agent intelligente e, opzionalmente, dell'intera infrastruttura IT aziendale, prendendo totalmente in gestione le piattaforme e soluzioni per la sicurezza o affiancando il team interno, se presente.

Il Servizio

Il servizio si adatta con flessibilità alle esigenze del Cliente e può essere personalizzato a seconda delle necessità e delle misure di sicurezza già presenti o da attuare. È garantita inoltre la drastica riduzione degli alert e dei falsi positivi da sistemi di terze parti (SIEM, SOC, ecc.) grazie alla fase di Incident Triage, durante la quale gli analisti di *ITC* valutano l'anomalia riscontrata. Il Cliente verrà contattato solamente in caso di incidente effettivo, per poi procedere alla successiva attività di Analisi e di Incident Response..

In particolare, la gestione esternalizzata della sicurezza può intervenire sui seguenti aspetti:

- Endpoint Security (installazione di agent intelligenti sui device dei dipendenti)
- Firewall & Proxy (per analisi delle configurazioni e "blocklist")
- Advanced Threat Protection systems (soluzioni anti-apt)
- Server DNS
- SIEM
- Sistemi eventuali da valutare

Il CyberSecurity Center di *ITC* risponde, inoltre, all'ingaggio da parte del cliente qualora si verifichino anomalie o sia necessario supporto tecnico qualificato. Rientra in questa casistica ogni richiesta attinente all'ambito della cybersecurity come, ad esempio, analisi di mail sospette, tentativi di phishing e download di file potenzialmente malevoli.

La tempestività dell'analisi forense post-incidente e della successiva bonifica dei sistemi per riprendere l'attività risulta essenziale, non solo per prevenire ingenti danni sia economici che d'immagine, ma anche in quanto necessaria alla compliance normativa a leggi italiane ed europee come il GDPR e la direttiva NIS (se applicabile). Nel caso in cui un incidente informatico sia anche causa di un Data Breach, i tempi previsti dalla legge per la segnalazione alle autorità competenti sono molto brevi e devono comprendere anche l'analisi dell'accaduto.

inthecyber
intelligence & defense advisors

InTheCyber Group SA
Via Vegezzi, 4 - 6900 Lugano, CH - T. +41 91 911 7 301

InTheCyber s.r.l.
Piazza Ernesto De Angeli, 3 - 20146 Milano, IT - T. +39 02 4801 3067

inthecyber
intelligence & defense advisors

InTheCyber Group SA
Via Vegezzi, 4 - 6900 Lugano, CH - T. +41 91 911 7 301

InTheCyber s.r.l.
Piazza Ernesto De Angeli, 3 - 20146 Milano, IT - T. +39 02 4801 3067