Wildix

SICUREZZA NELLE UNIFIED COMMUNICATIONS:
è possibile essere “Secure-by-Design?”

CONTENUTI

Wildix srl

Località le Basse, 3
38123 Trento, Italy
P.IVA IT01928890225

www.wildix.com
info@wildix.com
+39 0461 1715111

LA SICUREZZA COME NECESSITÀ

Senza alcun dubbio, in tutti i settori dell'IT la sicurezza è fondamentale. Sebbene ciò interessi sia il contesto dei consumatori sia quello delle aziende, la necessità di protezione dagli attacchi informatici è molto più elevata in un contesto aziendale, a causa del maggiore impatto di tali attacchi.

CIÒ È DOVUTO A DUE FATTORI PRIMARI:

1. **Subire un attacco informatico danneggia gravemente la reputazione di un'azienda,** facendo sì che partner commerciali ed i clienti si chiedano se possono affidare i propri dati personali ad un'azienda che di fatto non è protetta.

2. **I server aziendali detengono una quantità molto elevata di dati finanziari o sensibili che i criminali informatici possono sfruttare in molteplici modi.**

L'importanza di questi fattori può solo aumentare se si considera la frequenza con cui vengono effettuati gli attacchi informatici alle aziende.

- Da gennaio 2005 a marzo 2020 ci sono state 11.556 violazioni della sicurezza delle informazioni, con conseguente divulgazione di un totale di 1.663 trilioni di documenti.[1]
- Gli attacchi informatici sono costati **3 trilioni di dollari nel 2015** e costeranno **6 trilioni di dollari nel 2021.**
- La spesa mondiale per la sicurezza delle informazioni ha superato **114 miliardi di dollari nel 2018** e crescerà a **170,4 miliardi di dollari nel 2022.**
- **Nel 2018 il 92%** delle aziende nordamericane ha subito un attacco denial of service (DDoS). Questi attacchi sono costati alle aziende statunitensi un totale di oltre **10 miliardi di dollari all'anno.**
- **Il 28%** delle piccole imprese ha subito un attacco informatico. **Di conseguenza:**

69%

è stato temporaneamente offline

37%

ha subito una perdita finanziaria

25%

ha presentato istanza di fallimento

Citazione delle fonti a pagina 15

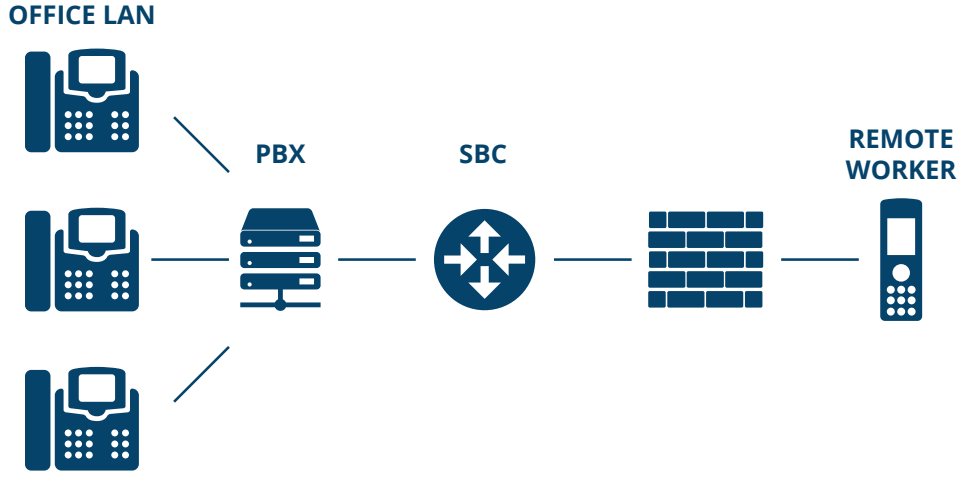
OPZIONI AL DI SOTTO DEGLI STANDARD

A causa di queste minacce alla reputazione e persino alle partecipazioni finanziarie dirette, **le aziende hanno un forte ed urgente bisogno di continuare ad investire nella sicurezza IT.**

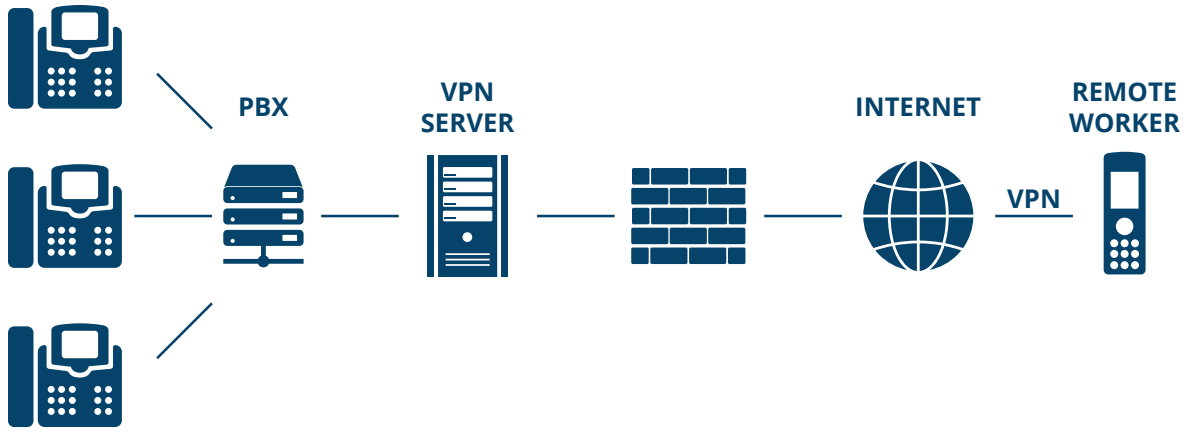
Tutto ciò si estende al settore delle Unified Communications, dove lo scambio di informazioni riservate internamente o esternamente può rendere chat, chiamate vocali e video un obiettivo redditizio per i criminali informatici.

Per combattere tali minacce, le aziende spesso utilizzano una delle due misure di sicurezza qui indicate, o entrambe:

- **SBC (Session Border Controllers):** un dispositivo distribuito su una connessione Internet per stabilire la sicurezza durante le sessioni (ossia una singola istanza di comunicazione tra due parti sulla rete). Funzionano come gateway metaforici che controllano il traffico di dati in entrata e in uscita da una rete VoIP, escludendo idealmente gli agenti dannosi come gli hacker. Di solito, gli SBC sono un elemento integrato nel router di rete o in qualche altra parte esterna alla piattaforma UCC stessa.



- **VPN (reti virtuali private):** una rete virtuale stabilita all'interno di una connessione pubblica. Queste connessioni creano un "tunnel" metaforico all'interno di una rete esistente, oltre a crittografare i dati in modo che non possano essere letti da utenti non autorizzati. Per accedere alle VPN è necessario loggarsi e ciò significa che, in teoria, la loro connessione è accessibile solo al personale autorizzato.



SUBSTANDARD OPTIONS

Tuttavia, **QUESTE DUE CONFIGURAZIONI, ANCHE SE MOLTO COMUNI, PRESENTANO DIVERSI PROBLEMI:**

- Poiché le VPN richiedono un login aggiuntivo, si crea **uno spazio aggiuntivo dove gli hacker possono accedere alle reti protette.** Vi è anche un **elevato rischio di errore da parte dell'utente,** poiché i dipendenti potrebbero rifiutarsi di utilizzarle durante le sessioni di comunicazione.

- **Le VPN in genere occupano una larghezza di banda aggiuntiva,** con alcuni codec come G.729 che richiedono il doppio del normale utilizzo della rete.

- Affidarsi a uno SBC per la sicurezza significa che **se quest'ultimo viene violato, non ci sono altre misure di sicurezza per fermare l'intrusione** e un attacco riuscito può diffondersi rapidamente su un intero server aziendale.

- Le VPN esterne e gli SBC devono essere gestiti in aggiunta alla stessa soluzione UCC, **aumentando il costo della manutenzione della sicurezza informatica e il lavoro ad essa associato. Anche il rischio di errore dell'utente o di guasto del dispositivo è elevato,** poiché se i tecnici o gli utenti finali commettono un errore con la misura di sicurezza, o se tali misure presentano qualche vulnerabilità, automaticamente nascono ulteriori modi in cui i criminali informatici possono entrare nella rete.

ALTERNATIVE PREFERIBILI

Per evitare i problemi creati da queste vulnerabilità intrinseche e dagli errori degli utenti, e ridurre i costi di sicurezza nelle UC nel loro insieme, **è preferibile implementare un'architettura UC che sia "secure-by-design".**

Questo assioma si riferisce a **un'implementazione di misure di sicurezza direttamente all'interno del PBX e su tutti i suoi dispositivi associati:** la rete, tutti i telefoni collegati, lo stesso software UC ed ogni singola licenza software.

Se ogni singolo elemento all'interno di una piattaforma UC ha le proprie misure di sicurezza, la sicurezza della rete nel suo complesso aumenta in modo significativo. Per cominciare, **la rete stessa sarebbe maggiormente protetta** grazie ai protocolli di sicurezza più solidi e completi che la salvaguardano. Inoltre, nel caso in cui la rete venisse violata, **tale intrusione si diffonderebbe più lentamente,** poiché ulteriori misure di sicurezza implementate su singoli dispositivi e istanze software bloccherebbero l'attacco invece di subirlo passivamente.

Se le misure di sicurezza fossero completamente integrate nella piattaforma, **non ci sarebbe bisogno di una manutenzione regolare da parte del personale IT o di formare i dipendenti contro un uso improprio,** e tutto ciò si tradurrebbe in una maggiore sicurezza. Di conseguenza, l'errore dell'utente e i vari rischi associati diminuirebbero drasticamente.

Vale anche la pena considerare che **questo approccio alla sicurezza ridurrebbe anche i costi associati,** poiché non vi sarebbero commissioni o pagamenti per un protocollo di sicurezza implementato separatamente.

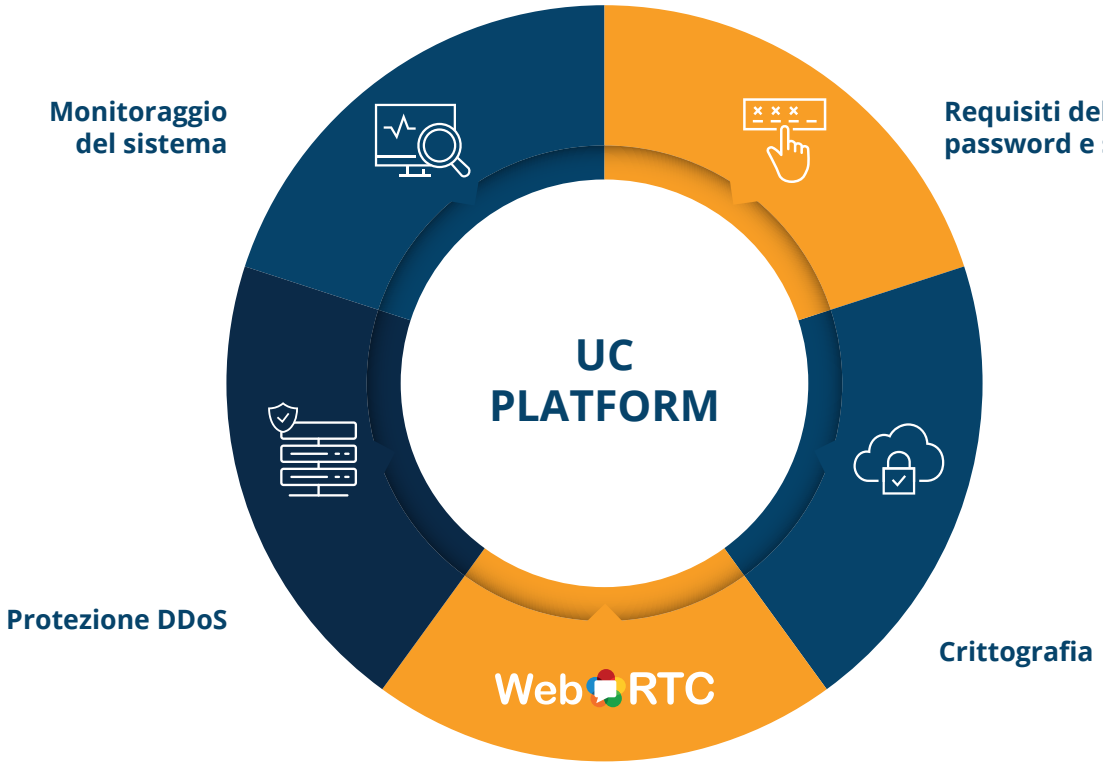
Wildix srl

Località le Basse, 3
38123 Trento, Italy
P.IVA IT01928890225

www.wildix.com
info@wildix.com
+39 0461 1715111

ELEMENTI DI
UNA PIATTAFORMA “SECURE-BY-DESIGN”

Parlando di cose concrete, l’implementazione di una piattaforma UC con misure efficaci integrate nella sua progettazione dovrebbe utilizzare i seguenti elementi protettivi:



Architettura WebRTC

QUESTI ELEMENTI SARANNO ANALIZZATI PIÙ NEL DETTAGLIO NELLE PAGINE SUCCESSIVE.

REQUISITI DELLA PASSWORD E SICUREZZA

In ogni aspetto della sicurezza informatica, le password sono un elemento essenziale. Ma ciò significa che **l'elemento protetto può essere tale solo se la password è sicura.** Gli hacker possono facilmente indovinare o dedurre password comuni e non complesse ("abc123," "password", ecc.), perciò **password scadenti fanno sì che la piattaforma UC possa essere facilmente preda di attacchi.**

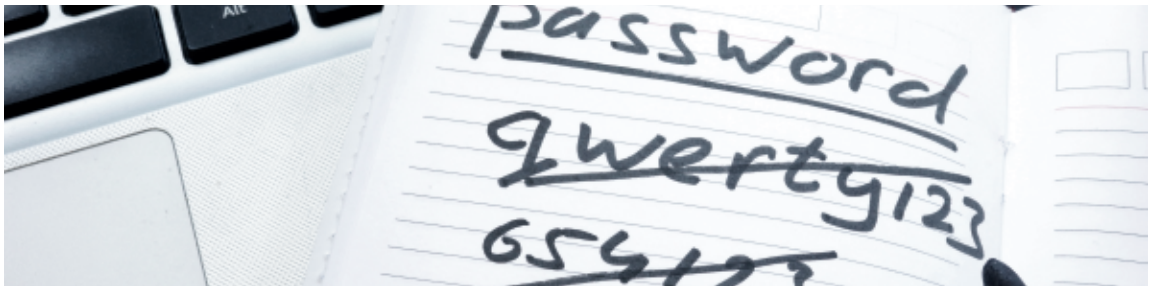
Per colmare questa lacuna, **una sicurezza efficace deve includere un requisito di password complesse.** Poiché molti utenti ignoreranno gli standard di sicurezza e proveranno a creare una password facile da ricordare (ma poco sicura), **il sistema deve richiedere necessariamente una password complessa:** quando si configura un account, il sistema stesso dovrebbe chiedere agli utenti di creare una password con più caratteri, numeri e simboli univoci ("@", "^", ecc.) e rifiutare eventuali password che non soddisfano gli standard di complessità.

Inoltre, **le password dovranno essere salvate in modo sicuro e crittografato per garantire che siano inutilizzabili in caso di accesso illecito al server.** Ciò può essere fatto rapidamente ed efficacemente utilizzando l'algoritmo SHA512 e la crittografia salt, due metodi di crittografia che randomizzano efficacemente i dati di ingresso in modo che solo il server interno possa decodificarli.

Oltre a questa protezione, **il sistema deve proteggere dai tentativi di accesso "brute force"**, in cui gli intrusi passano in rassegna i caratteri in modo casuale ed eseguono più tentativi di accesso. Questo obiettivo può essere raggiunto in modo efficace configurando il sistema in modo da **negare l'accesso a qualsiasi indirizzo IP che effettui un numero eccessivo di tentativi falliti in un breve periodo di tempo.** Tali istanze e i relativi indirizzi IP correlati dovrebbero inoltre essere registrati dal sistema per essere esaminati da un admin.

Per una maggiore sicurezza dell'accesso, il sistema dovrebbe includere anche l'opzione per **l'autenticazione a 2 fattori (2FA),** dove oltre a inserire una password, gli utenti devono inserire anche un codice una tantum, generato casualmente, inviato alla loro e-mail o al loro dispositivo personale. Tale requisito aggiuntivo riduce drasticamente il rischio di attacchi agli account, poiché un hacker dovrebbe avere accesso alla posta elettronica o all'istanza specifica dell'utente del software di generazione del codice per l'accesso.

In alternativa, un modo per ridurre il rischio di errore dell'utente nella protezione della password è l'implementazione di un protocollo **Single Sign-On.** In questo processo, gli utenti possono semplicemente accedere al proprio account PBX inserendo il nome utente e la password di un altro account, come quello Gmail o Microsoft. Questa procedura **migliora la sicurezza grazie alla sua praticità:** se gli utenti devono ricordare numerose password complesse, il rischio che lascino le password facilmente accessibili (ad esempio scritte su un foglio di carta) per paura di dimenticarle è molto elevato. Ecco perché realisticamente è meglio fare in modo che gli utenti debbano ricordare solo una password altamente sicura. La procedura di Single Sign-On dovrebbe essere utilizzata anche in modo combinato con 2FA, per una maggiore sicurezza.



CRITTOGRAFIA

Poiché molti hacker e attacchi informatici operano intercettando efficacemente le comunicazioni in corso, anziché semplicemente accedere agli account, è essenziale che tali comunicazioni siano crittografate. Lo scopo è più o meno lo stesso di una VPN: **anche se soggetti non autorizzati accedono ai dati trasmessi, tali dati sono in uno stato in cui non possono essere utilizzati.**

Per impostazione predefinita, **il sistema dovrebbe utilizzare Transport Layer Security (TLS) per crittografare i dati tra utenti:** questo sistema funziona condividendo un metodo di decrittografia solo tra utenti diretti e utilizzando un autenticatore di certificati di terze parti (CA) per verificare l'identità di entrambi gli utenti. In altre parole, **utilizzando il sistema TLS, i dati vengono crittografati tramite una crittografia nota solo agli utenti coinvolti, rendendo impossibile la decifrazione agli utenti non autorizzati.** In una configurazione ideale, TLS verrebbe utilizzato per voce, video, condivisione dello schermo, messaggi e qualsiasi altra comunicazione avviata tramite il PBX.

Il sistema dovrebbe anche utilizzare il Secure Real-Time Protocol (SRTP), uno standard per la trasmissione dei dati sul web con ulteriore crittografia e autenticazione. Simile a TLS, **trasforma le comunicazioni in dati codificati, quindi identifica l'utente giusto a cui assegnare le chiavi di decodifica.** Un modo particolarmente efficace per implementare questo protocollo è tramite la chiave SDES-AES 128 e la chiave DTLS-SRTP (che funziona direttamente insieme a TLS), per un'ulteriore crittografia di tutte le comunicazioni.

Ribadendo il concetto, sebbene un processo di crittografia da solo non possa impedire ad utenti non autorizzati di intercettare le comunicazioni, è comunque una parte cruciale della creazione di una piattaforma "secure-by-design". Implementata correttamente, **la crittografia garantisce che, anche ottenuto ottengono l'accesso al funzionamento interno del sistema, non si possa fare un uso pratico dei dati scoperti:** questo crea un elevato livello di sicurezza intrinseco nella progettazione del sistema.

Wildix Collaboration

PROTEZIONE DDOS

Come detto in precedenza, **gli attacchi DDoS sono di primaria importanza per la struttura della sicurezza di qualsiasi azienda.** Tali attacchi si verificano quando una quantità volutamente eccessiva di traffico web viene indirizzata a un singolo server web allo scopo di sovraccaricarlo e causarne l'arresto anomalo. Poiché tali attacchi possono anche essere indirizzati ai server UC, un'adeguata configurazione della sicurezza deve implementare protezioni contro tali eventualità.

Questa protezione sarebbe già in parte realizzata dall'elemento precedentemente considerato di protezione da attacchi "brute force", in cui troppi tentativi di password errata bloccano l'accesso da un indirizzo IP. Questa protezione garantirebbe già che un utente malintenzionato non possa sovraccaricare il sistema costringendolo ad elaborare un eccesso di tentativi di password errate.

Ma sarebbe necessario tutelarsi con un'ulteriore protezione. Il sistema stesso deve disporre di **un protocollo che gestisca il traffico in entrata nel sistema** (sia interno che esterno) al fine di garantire che i dati non sovraccarichino il sistema tramite chiamate vocali, videoconferenze, messaggistica istantanea o qualsiasi altra funzionalità integrata nel sistema.

Simile alla protezione da attacchi "brute force", questo sistema potrebbe facilmente funzionare come **una disposizione che blocca completamente il traffico da un IP se i dati sono in una quantità tale da minacciare di sovraccaricare il server.** Infatti, considerando la realtà e la gravità del rischio rappresentato dagli attacchi DDoS, tale misura non è un'opzione: è anzi assolutamente necessaria per un sistema UC completamente sicuro, in particolare uno che può affermare di avere la sicurezza integrata nella propria struttura fondamentale.

Sistema UC di Wildix: la sicurezza è integrata nella sua architettura.

Wildix srl

Località le Basse, 3
38123 Trento, Italy
P.IVA IT01928890225

www.wildix.com
info@wildix.com
+39 0461 1715111

Una fonte meno ovvia di sicurezza web all'interno di UC proviene da **WebRTC** (Web Real-Time Communication), un framework di comunicazioni Internet che arriva integrato nella maggior parte dei moderni web browser. Un progetto Open Source basato su HTML 5 e JavaScript e avviato da Google nel 2011, la cui tecnologia è costituita da una serie di protocolli e interfacce che consentono comunicazioni istantanee e sicure tra browser web compatibili.

Dal punto di vista della sicurezza, **WebRTC offre numerosi vantaggi chiave rispetto ad altri protocolli di comunicazione,** sia in termini di sicurezza attiva che di prevenzione degli errori dell'utente.

Innanzitutto, **WebRTC non funziona tramite plug-in o software esterni, ma internamente tramite un browser.** Pertanto, **WebRTC viene aggiornato rapidamente e automaticamente e non si basa sull'input dell'utente per passare alla versione più recente.** Ciò garantisce che l'errore dell'utente non comporti l'utilizzo del sistema con una vulnerabilità senza patch.

Inoltre, poiché WebRTC opera attraverso il browser anziché tramite un plug-in a parte, **il protocollo non è influenzato da vulnerabilità di sicurezza che possono invece esistere sul dispositivo di un singolo utente.** Se, ad esempio, il laptop di lavoro di un utente è stato infettato da spyware, non c'è modo per il programma di raggiungere l'istanza di WebRTC, in quanto non "esiste" realmente sul laptop e non può essere infettato. Di conseguenza, agli utenti viene garantita la navigazione sicura anche se utilizzano dispositivi personali (e potenzialmente compromessi).

WebRTC implementa anche le seguenti misure di sicurezza specifiche:

- **Richiede l'autorizzazione esplicita dell'utente per utilizzare la webcam o il microfono** e mostra attivamente all'utente quando tali dispositivi sono in uso, il che significa che non c'è modo per hacker o programmi di dirottare la webcam o il microfono attraverso la tecnologia

- **Offre una crittografia end-to-end completa tramite DTLS e SRTP**,che non vengono mai decrittografati durante la connessione: in altre parole, anche se le comunicazioni fossero intercettate da terzi, non sarebbero decifrabili dall'interceptor

- **Le connessioni WebRTC vengono effettuate direttamente da browser a browser,** senza intermediari, ovviando alla possibilità di intercettazione

Inoltre, poiché questi elementi di WebRTC sono intrinsecamente integrati nel browser, la loro implementazione potrebbe essere facilmente un processo automatico. Ciò garantirebbe ancora una volta che la sicurezza per il sistema UC sia un aspetto intrinseco della piattaforma, piuttosto che qualcosa da gestire esternamente.

MONITORAGGIO DEL SISTEMA

Infine, **è fondamentale che gli amministratori abbiano una capacità completa di monitorare il sistema UC,** poiché anche le piattaforme più sicure hanno comunque un rischio di intrusione e dovrebbero quindi disporre di mezzi per rilevare tali istanze in dettaglio.

Pertanto, un'efficace piattaforma di sicurezza UC (in particolare una con sicurezza intrinseca) deve includere anche **avvisi automatici di intrusioni di sistema su tutti i dispositivi gestiti dal PBX,** nonché avvisi di eventuali attacchi che hanno origine all'interno del sistema (ad esempio, l'account di un utente autorizzato utilizzato per un attacco DDoS).

Per ulteriori approfondimenti opzionali, **il sistema dovrebbe anche includere l'integrazione con un software di monitoraggio esterno, come Zabbix.** Ciò consentirebbe al personale addetto alla sicurezza di fornire maggiori dettagli e di segnalare eventuali attacchi rilevati o vulnerabilità nel sistema.

Wildix srl

Località le Basse, 3
38123 Trento, Italy
P.IVA IT01928890225

www.wildix.com
info@wildix.com
+39 0461 1715111

CASI D'USO

Per illustrare in modo più pratico il vantaggio combinato di questi vari elementi, in questa sezione verranno elencati una serie di casi ipotetici della loro implementazione. Per un quadro più completo del loro scopo e valore, ogni caso indicherà uno scenario che si svolge **con e senza l'elemento di sicurezza specifico.**

1. Un attacco DDoS colpisce un sistema attraverso più tentativi di accesso.

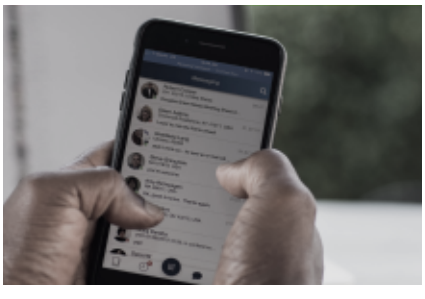
NON "SECURE BY DESIGN": il sistema è sovraccarico e **tutti sono chiusi fuori** per un periodo di tempo che va da mezz'ora a più ore.

SECURE BY DESIGN: dopo un numero limitato di tentativi di accesso, **l'utente malintenzionato viene bloccato.** L'attacco viene registrato nel sistema per consentire a un amministratore di esaminarlo e difendersi da esso.

2. Un utente finale sta configurando un account su un PBX. Ignorando il protocollo aziendale, decide di creare una password breve e semplice, con la scusa che sarà facile da ricordare.

NON "SECURE BY DESIGN": l'utente è autorizzato a creare la password di base. Poco dopo, **un hacker che ha accesso al suo nome utente indovina rapidamente la semplice password** e blocca l'utente fuori dal suo account.

SECURE BY DESIGN: il sistema impedisce attivamente all'utente di creare la password semplice e **lo costringe a crearne una complessa.** Sebbene l'utente sia frustrato dal fatto di dover utilizzare una password complessa, scopre la funzione di single sign-on, che gli consente di accedere con una password complessa che ha già memorizzato.



3. Adam vuole inviare un breve messaggio alla sua collega, Brenda, per chiedere informazioni sulle finanze.

NON "SECURE BY DESIGN": il sistema UC è protetto da una VPN, a cui Adam dovrebbe accedere per tutte le comunicazioni. Tuttavia, poiché è un messaggio rapido, **Adam decide che l'accesso alla VPN è troppo complicato** e invia il messaggio senza protezione VPN. Quando il messaggio viene inviato, tuttavia, **i dati non crittografati vengono rubati da un hacker** che era a conoscenza dell'uso della VPN e in attesa di una falla nel sistema.

SECURE BY DESIGN: Adam non è tenuto ad accedere a una VPN per inviare questo messaggio. **È invece crittografato automaticamente, il che significa che anche se ci fosse un hacker che sta osservando la rete, non sarebbe comunque in grado di leggere le comunicazioni.**

4. Un utente finale deve comunicare immediatamente con un team su un progetto vitale che riguarda numerosi dettagli interni. La necessità di collaborare è così urgente che non ha tempo per gli aggiornamenti del suo PBX.

NON "SECURE BY DESIGN": l'utente finale accede al PBX senza scaricare un aggiornamento del firmware per il proprio SBC. Poiché **questo aggiornamento conteneva una patch per una vulnerabilità con SBC,** le comunicazioni dell'utente finale sono ora **aperte agli hacker.**

SECURE BY DESIGN: Web RTC è stato **aggiornato automaticamente** all'ultima versione più sicura immediatamente al momento dell'accesso dell'utente finale. L'utente può così comunicare con il suo team in **modo rapido e sicuro.**

5. Un cliente chiama un'azienda per interagire con un agente di chiamata. Si discute di molti dei dettagli privati del cliente, tra cui le informazioni di accesso al sito web della sua azienda e le informazioni bancarie.

NON "SECURE BY DESIGN": la conversazione si svolge tramite una VPN o SBC. Tuttavia, **la connessione non è protetta da parte del cliente.** Ecco quindi che un hacker che ha monitorato il cliente riesce ad **accedere direttamente ai suoi dati.**

SECURE BY DESIGN: la conversazione avviene tramite WebRTC condotta **direttamente dall'agente di chiamata al cliente e non può essere intercettata.** La conversazione è quindi **crittografata e viene garantita un'ulteriore protezione.**

Wildix srl

Località le Basse, 3
38123 Trento, Italy
P.IVA IT01928890225

www.wildix.com
info@wildix.com
+39 0461 1715111

VALORE OTTENUTO

Implementando queste misure di sicurezza, le aziende possono raggiungere **un equilibrio ideale tra sicurezza e usabilità.** Da un lato, avranno **un sistema posizionato in modo univoco per proteggersi dagli attacchi,** che sia in grado di difenderle da danni alla loro reputazione causati dalle violazioni e dagli elevati costi finanziari che tali attacchi comportano. Allo stesso tempo, gli utenti avranno accesso a **un sistema che rimane facile da implementare nella loro attività di tutti i giorni,** vale a dire un sistema che non è appesantito dall'attuazione della sicurezza.

Infatti, vale la pena considerare che quest'ultimo punto sull'usabilità stessa aumenta la sicurezza del sistema. Come mostrato dai casi d'uso, **se un utente finale ritiene che le misure di sicurezza siano eccessive o comunque un ostacolo al proprio lavoro, in genere troverà un modo per aggirare tali protocolli.** È quindi più utile che la sicurezza sia applicata senza problemi all'interno del design intrinseco della piattaforma, come illustrato nei principi delineati in precedenza.

Inoltre, **un sistema del genere porterebbe quasi sicuramente a un risparmio di denaro da parte delle aziende,** anche nel caso in cui non si verifichino attacchi informatici, in quanto con un sistema di sicurezza che non si basa su programmi esterni, verrebbero automaticamente spesi meno tempo e denaro nella manutenzione.

In breve, un sistema "secure-by-design", come precedentemente descritto, garantirebbe alle aziende **maggiore sicurezza, maggiore usabilità e meno spese.**

Data questa ricchezza di vantaggi, soprattutto rispetto ad altre opzioni leader sul mercato, **un tale sistema è senza dubbio un elemento di vitale importanza che qualsiasi azienda dovrebbe cercare nella propria piattaforma UC.**

Citando fonti:

bit.ly/Security-in-UCC

bit.ly/Security-in-UCC-2

bit.ly/Security-in-UCC-3

bit.ly/Security-in-UCC-4

bit.ly/Security-in-UCC-5

Desideri maggiori informazioni sulla sicurezza nelle UC?
Visita il nostro sito web

www.wildix.com

per vedere il nostro prodotto, Wildix, e scoprire come implementa questi principi in situazioni aziendali reali.


T-Mobile
9:31 AM
91%
Messaging
Robert Cooper
OH 43065, United States
08:47
Douglas Green Media Briefing Sheet.d...
Dawn Adkins
Cincinnati Roadshow, KY 41011, USA
31.07.19
I want to ride the Ferris wheel!
Anastasia Lang
Ukraine, 65000
31.07.19
yeah I think so - he sent an e-mail wit...
Steve Grinsztein
MA 01879, USA
31.07.19
you're welcome
Amy Richwagen
WA 98671, USA
31.07.19
OK, good to know. Thanks again.
Philip Turkov
Cincinnati RS, OH 43215, USA
31.07.19
thanks!
Giulia Perotta
08005 Barcelona, Spain
yep!
Dara Hill
Ukraine, 65000

Wildix