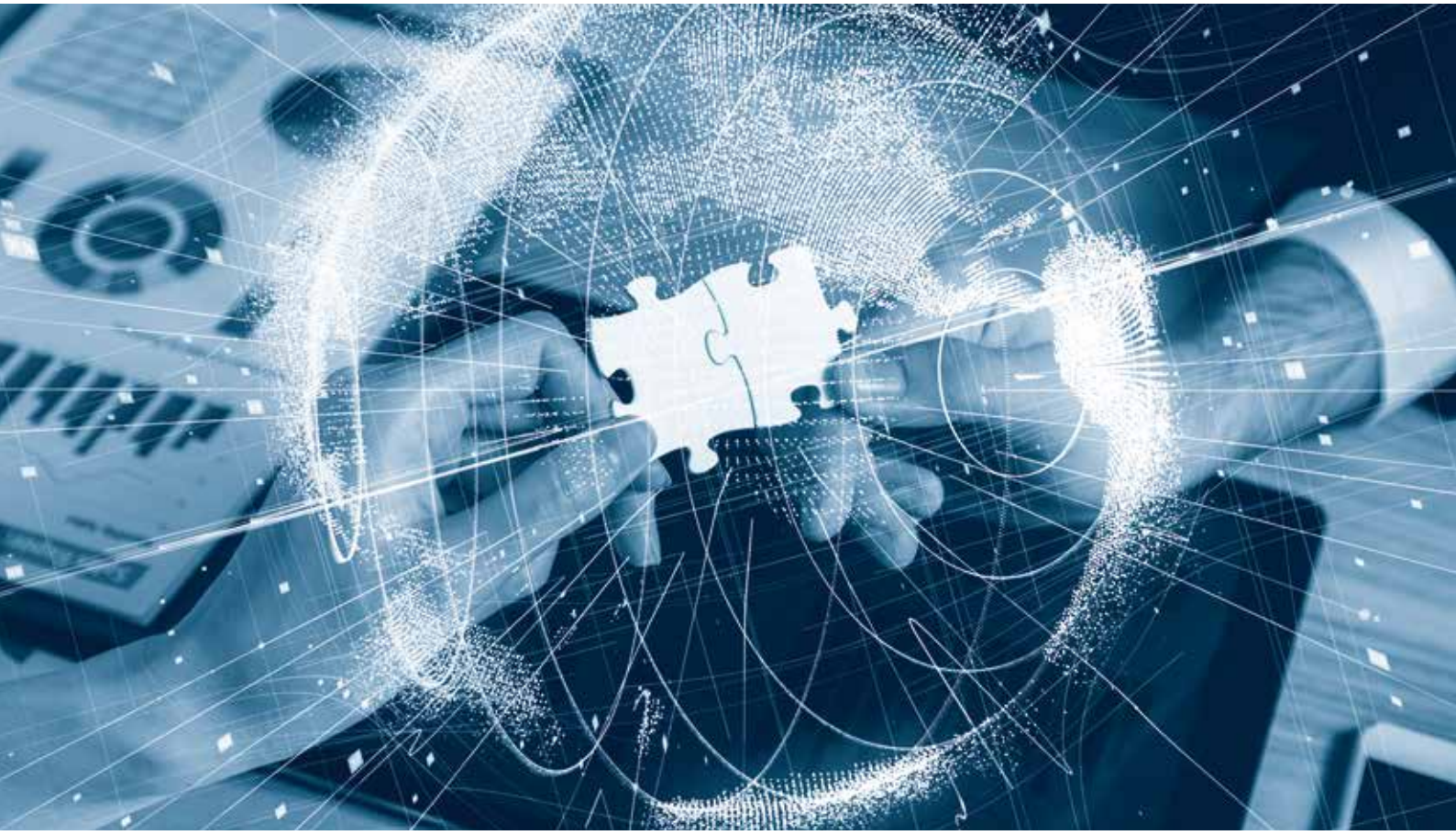
eCall
Business
Messaging

Ecco come eCall protegge i vostri dati dagli hacker

L‘autenticazione a due fattori



Ecco come eCall protegge i vostri dati dagli hacker

eCall Business Messaging

Sono considerate il principale fattore di rischio nella sicurezza informatica: le password I criminali informatici riescono sempre più spesso a fare irruzione nelle banche dati causando gravi danni [1]. L'autenticazione a due fattori di eCall vi aiuta a proteggere efficacemente i vostri dati aziendali sensibili.

1 https://www.searchsecurity.de/meinung/Passwoerter-Der-groesste-Risikofaktor-in-der-IT-Sicherheit

Le aziende investono molto denaro nelle tecnologie più all'avanguardiaper proteggere la loro infrastruttura informatica e i loro dati dagli accessi non autorizzati. Spesso, però, il punto debole non sono le tecnologie utilizzate ma le persone. Sempre più spesso gli attacchi avvengono a causa di errori degli utenti, ad esempio una scelta di password poco sicure o la conservazione di passwordin modo inappropriato. Non è una novità, vero?

Un rischio per la sicurezza: la persona

A chi non è mai successo? Post-it con password sotto l'agenda o persino appiccicati allo schermo sotto gli occhi di tutti. Nella scelta delle password si usano combinazioni di numeri o di cifre semplici da ricordare.
O peggio: la stessa semplice password viene utilizzata per vari servizi online. Non è una brutta abitudine del passato, a è un modo di fare più attuale che mai. Lo dimostra anche la Top 10 delle password più utilizzate in Germania, secondo le rilevazioni dell'Hasso Plattner Institut (HPI). Come base dati sono stati utilizzati 12,9 milioni di indirizzi e-mail «.de».

Vincitrice indiscussa del 2017: 123456

Classifica	Password
1	123456
2	123456789
3	1234
4	12345
5	12345678
6	hallo
7	passwort
8	1234567
9	111111
10	Hallo123

Fonte: https://hpi.de/pressemitteilungen/2017/die-top-ten-deutscher-passwoerter.html

L'effetto domino e le relative conseguenze possono causare, in caso di attacco, gravi danni.

Social Engineering – Un attacco alla psicologia dell'utente

Anche quando si usano le password in modo professionale e responsabile non si possono escludere i furti i dati e identità. I criminali informatici utilizzano spesso e volentieri «trucchetti» psicologici per sfruttare i punti deboli degli utenti. Con mail di phishing, chiamate di vishing (Voice Phishing) e altri attacchi i collaboratori vengono consapevolmente manipolati o ingannati per fargli fornire «volontariamente» dati o password sensibili agli hacker. Tutti questi metodi sono stati raccolti sotto il termine generico di Social Engineering.

Un clic di troppo

Anche l'utilizzo del malware è una modalità molto diffusa per arrivare ai dati di accesso confidenziali degli utenti. Basta cliccare su un link «nocivo» in un'e-mail e l'utente installa senza accorgersene un malware nel computer. In questo modo è possibile ad esempio registrare tramite keylogger i tasti digitati dall'utente e successivamente leggerli. Secondo uno studio attuale condotto da scienziati statunitensi ormai basta una termocamera per rilevare le password attraverso le tracce di calore sulle tastiere.

Particolarmente semplici da leggere sono i tasti digitati dagli utenti poco esperti e lenti nell'uso della tastiera. La crescente digitalizzazione richiede quindi nuove disposizioni di legge, primo fra tutti il Regolamento generale sulla protezione dei dati dell'Unione europea (GDPR), e metodi di autenticazione sicuri per proteggere efficacemente i dati di aziende, clienti e collaboratori.

eCall
Business
Messaging

Ecco come eCall protegge i vostri dati dagli hacker

Più sicurezza con un sistema di autenticazione a due fattori
Un metodo diffuso e consolidato per proteggere gli accessi e i login in Internet da accessi non autorizzati è l'autenticazione a due fattori. In questo modo viene creata un'ulteriore barriera contro le truffe. Oltre all'inserimento di un nome utente e di una password, l'utente deve identificarsi con un ulteriore elemento sotto forma di codice o token. Anche se i dati di accesso sono già finiti nelle mani sbagliate, con queste ulteriori caratteristiche di autenticazione è possibile impedire i tentativi di frode online.

Codici di accesso via SMS e messaggi vocali sul cellulare
La soluzione Software-as-a-Service (SaaS) di eCall vi aiuta a fare in modo che l'informazione giusta arrivi alla persona giusta al momento giusto! Con l'utilizzo di numeri di transazione mobile (mTAN) si possono inviare agli utenti autorizzati codici di accesso tramite SMS o messaggio vocale. Questa funzione protegge meglio voi e i vostri utenti dai furti di dati. Per le informazioni molto sensibili si consiglia l'opzione «High Privacy», con la quale il sistema provvede a sovrascrivere tutti i contenuti dopo l'elaborazione. Questa opzione è pensata soprattutto per i settori che gestiscono dati molto sensibili, per esempio Finance & Banking, settore sanitario e assicurazioni. Dopo l'invio non è più possibile ricostruire l'SMS originale.

I buoni motivi per scegliere l'autenticazione a due fattori mediante SMS

- I nomi utenti e le password non sono più abbastanza sicuri
- Il Regolamento sulla protezione dei dati personali dell'UE impone autenticazioni sicure
- Al giorno d'oggi praticamente ciascuno possiede un cellulare e può quindi ricevere SMS. Quindi, eCall può essere implementato come soluzione SaaS semplice e conveniente nell'infrastruttura IT esistente
- Collegamento semplice alle interfacce (API) e ai software di fornitori globali come RSA SecurID Appliance, SMS Passcode (mediante Web service) e SafeNet (con HTTPS)
- Affidabilità assoluta, elevata disponibilità e trasmissione rapida dei messaggi
- Elevata qualità di spedizione sul territorio nazionale e all'estero grazie all'«SMSRouting-Finder»
- Fornitore leader di Business Messaging in Svizzera

Convincetevene voi stessi. Effettuate un test gratuito
e non vincolante mediante www.ecall.ch.

F24 – Il vostro partner solido per i sistemi di segnalazione, di gestione delle crisi e della comunicazione aziendale di livello critico.

F24 è il più rinnomato fornitore in Europa di software-as-a-service per sistemi di segnalazione e di gestione delle crisi (FACT24) e per la comunicazione di dati sensibili e di livello critico. Con FACT24, F24 offre ai clienti di tutto il mondo una soluzione altamente innovativa per la gestione ottimale dei casi di emergenza e di crisi o in generale di elevato livello di criticità. In qualità di primo e unico fornitore non americano, F24 è citata nell'elenco dell›attuale report Gartner per i servizi di notifica in caso di emergenza e di messaggistica di massa (in inglese EMNS).

Con la sede principale a Monaco di Baviera, l'azienda risponde alle direttive tedesche in materia di protezione dei dati e l'hosting del suo sistema SaaS FACT24 avviene esclusivamente in centri di calcolo tedeschi. F24 offre inoltre protezione aggiuntiva a clienti di FACT24 sia nazionali che internazionali grazie a numerose altre misure. FACT24 permette alle aziende di affrontare al meglio e a 360 gradi le situazioni di pericolo, senza ovviamente trascurare gli aspetti legati alla sicurezza e alla protezione dei dati.

Da aprile 2016, Dolphin Systems AG con sede a Wollerau fa parte del gruppo F24. A partire da ottobre 2019 è stata rinominata F24 Schweiz AG. Con eCall l'azienda vanta 25 anni di esperienza nella realizzazione di soluzioni IT e di telecomunicazione sul mercato svizzero. Con questa piattaforma, F24 offre in particolare soluzioni per la comunicazione di grandi volumi di dati di carattere critico e riservato in ambiente aziendale.

Per ulteriori informazioni, non esitate a contattarci in qualsiasi momento o visitate il nostro sito web www.f24.com.

F24 WWW.F24.COM

F24 Schweiz AG
Samstagernstrasse 45
8832 Wollerau, Svizzera

T +41 44 787 30 70
F +41 44 787 30 71
office_ch@f24.com