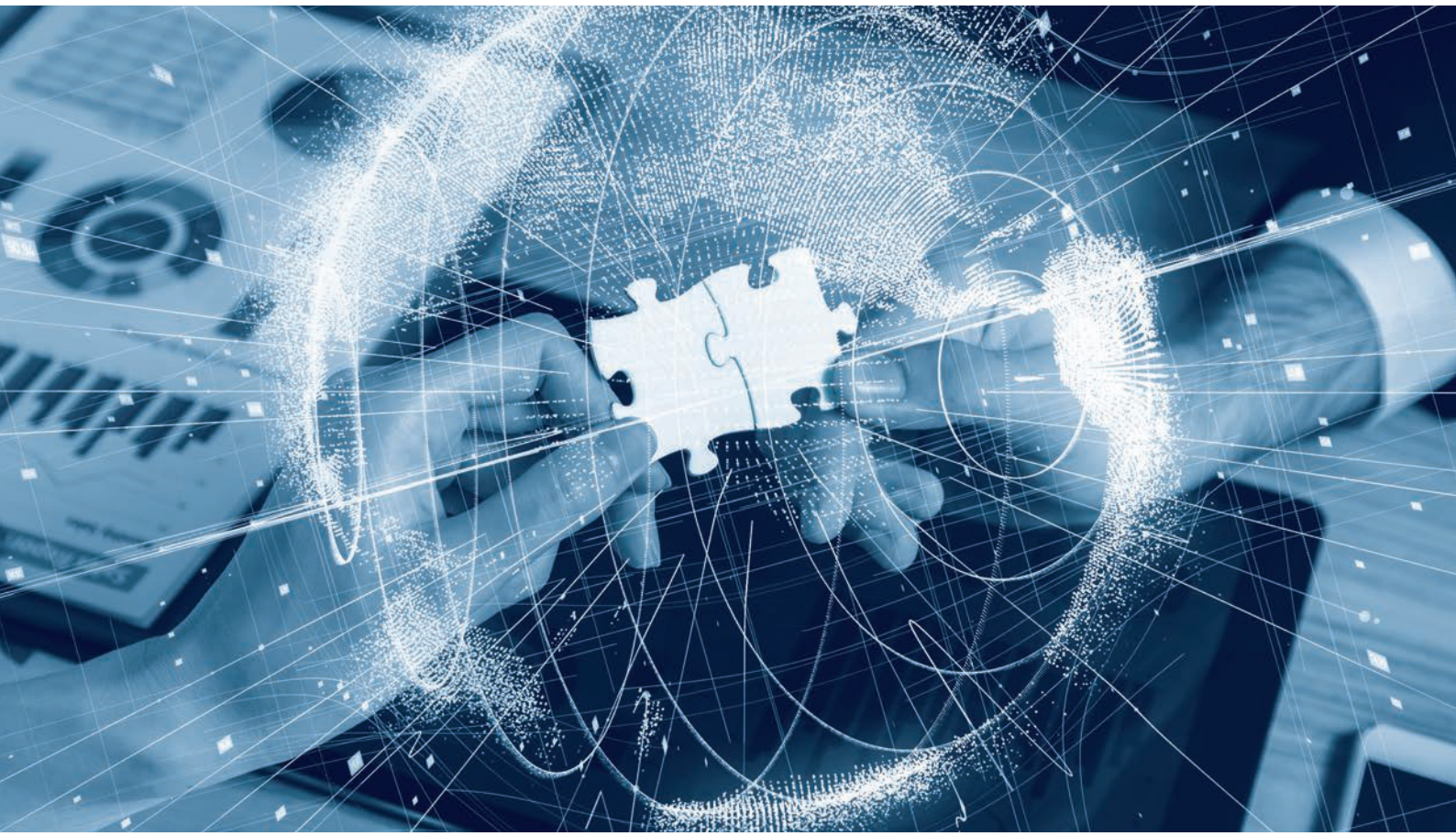
eCall
Business
Messaging

So schützt eCall Ihre Daten vor Hackern

Zwei-Faktor-Authentifizierung



eCall ist ein Produkt von
Dolphin Systems AG.
www.dolphin.ch

DOLPHIN
an F24 company

Weitere Informationen unter
www.ecall.ch

eCall
Business
Messaging

So schützt eCall Ihre Daten vor Hackern

Sie gelten als der grösste Risikofaktor in der IT-Sicherheit: Passwörter. Immer wieder gelingt es Cyberkriminellen, in Datenbanken einzubrechen und so grossen Schaden zu verursachen[1]. Die Zwei-Faktor-Authentifizierung von eCall hilft Ihnen sensible Unternehmensdaten effektiv zu schützen.

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

Unternehmen investieren viel Geld in aktuelle Technologien um Ihre IT-Infrastruktur und Daten vor unberechtigten Zugriffen zu schützen. Doch oftmals sind nicht die eingesetzten Technologien die Schwachstelle, sondern der Mensch selber. Immer häufiger erfolgen Angriffe aufgrund von Benutzerfehlern, zum Beispiel durch die Wahl unsicherer Passwörtern oder unsachgemässer Aufbewahrung von Kennwörtern. Keine neuen Erkenntnisse, oder doch?

Sicherheitsrisiko Mensch

Wer kennt das nicht? Haftnotizen mit Kennwörtern unter der Schreibunterlage oder teilweise sogar am Bildschirm gut sichtbar angeklebt. Bei der Auswahl von Kennwörtern nimmt man einfach zu merkende Zahlen-/Wortkombinationen.
Noch schlimmer: Dasselbe schwache Passwort wird für verschiedene Online-Diensten eingesetzt. Keine Situation aus der Vergangenheit, sondern der Status Quo. Dies zeigen auch die Top 10 der meistgenutzten Passwörter in Deutschland, ermittelt durch das Hasso-Plattner-Institut (HPI). Als Datengrundlage dienten hierzu 12.9 Millionen «.de»-E-Mail-Adressen.

Unangefochtener Sieger per 2017: 123456

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

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

Der Domino-Effekt und die daraus entstehenden Folgen können im Falle eines Angriffs grosse Schäden anrichten.

Social Engineering – Griff in die psychologische Trickkiste

Selbst bei einem professionellen sowie verantwortungsvollen Umgang mit Passwörtern sind Daten- und Identitätsdiebstähle nicht auszuschliessen. Hierzu greifen Cyberkriminelle gerne in die psychologische «Trickkiste» und nutzen gezielt Schwächen der User aus. Mit Phishing-Mails, Vishing-Anrufen (Voice Phishing) und anderen Angriffen werden Mitarbeiter bewusst manipuliert oder getäuscht, mit dem Ziel, dass diese «freiwillig» sensible Daten oder Passwörter dem Angreifer überlassen. All diese Methoden werden unter dem Begriff Social Engineering zusammengefasst.

Ein Klick zu viel

Doch auch die Nutzung von Malware ist eine weitverbreitete Art, um an vertrauliche Zugangsdaten von Nutzern zu gelangen. Ein Klick auf einen «bösartigen» Link in einer E-Mail reicht, um vom Benutzer unbemerkt bösartige Software auf einem Rechner zu installieren! Danach können beispielsweise mit einem Keylogger Tastatureingaben der User protokolliert und später ausgelesen werden. Gemäss einer aktuellen Studie von US-Wissenschaftlern, reicht mittlerweile sogar eine Wärmebildkamera, um über Wärmespuren auf Tastaturen Passwörter abzugreifen. Besonders leicht sind Eingaben von Nutzern des Zwei-Finger-Suchsystems auslesbar.

Deshalb erfordert die zunehmende Digitalisierung und neue gesetzliche Vorgaben, allen voran die EU-Datenschutzverordnung (DSGVO), sichere Authentifizierungsmethoden, um Daten von Unternehmen, Kunden und Mitarbeitern wirksam zu schützen.

eCall
Business
Messaging

So schützt eCall Ihre Daten vor Hackern

Mehr Sicherheit mit einer Zwei-Faktor-Authentifizierung
Eine gängige und bewährte Methode ist eine Zwei-Faktor-Authentifizierung um Zugänge und Logins im Internet vor unberechtigten Zugriffen zu schützen. Hierbei wird eine zusätzliche Schranke gegen Betrug eingerichtet. Neben der Eingabe eines Benutzernamens und eines Passworts muss sich der Nutzer mit einer weiteren Komponente in Form eines Codes oder Tokens identifizieren. Auch wenn Zugangsdaten bereits in falsche Hände geraten sind, können mit diesen zusätzlichen Authentifizierungsmerkmalen Online-Betrugsversuche unterbunden werden.

Zugangscodes per SMS und Sprachnachrichten auf Mobiltelefone versenden
Die Software-as-a-Service (SaaS) Lösung eCall unterstützt Sie dabei, dass die richtige Information zur richtigen Zeit bei der richtigen Person ankommt! Mit der Nutzung mobiler Transaktionsnummern (mTAN) können den befugten Usern Zugangscodes per SMS oder Sprachnachricht zugestellt werden. Diese Funktion schützt Sie und Ihre User besser vor Datendiebstahl. Für hochsensible Informationen empfiehlt sich die Option «High Privacy», wodurch sämtliche Inhalte nach der Verarbeitung vom System überschrieben werden. Diese Option eignet sich besonders für Branchen, die hochsensitive Daten verwalten wie beispielsweise Finance & Banking, Gesundheitswesen aber auch Versicherungen. Eine Rekonstruktion der originalen SMS ist nach Versand nicht mehr möglich.

Gute Gründe für eine Zwei-Faktor-Authentifizierung per SMS

- Benutzernamen und Passwörter sind nicht mehr sicher genug
- Die EU-Datenschutzverordnung erfordert sichere Authentifizierungsmöglichkeiten
- Heutzutage besitzt praktisch jede Person ein Mobiltelefon und kann damit SMS empfangen. Daher, kann eCall als kostengünstige und einfache SaaS-Lösung in bestehende IT-Infrastruktur implementiert werden
- Einfache Anbindung an Schnittstellen (API) sowie an Software globaler Anbieter wie RSA SecurID Appliance, SMS Passcode (via Webservice) und SafeNet (via HTTPS)
- Absolute Zuverlässigkeit, hohe Verfügbarkeit und schnelle Übermittlung der Nachrichten
- Hohe Versandqualität im In- und Ausland durch den «SMS-Routing-Finder»
- Führender Business-Messaging Anbieter in der Schweiz

Überzeugen Sie sich selbst. Testen Sie kostenlos und unverbindlich via www.ecall.ch.

Dolphin Systems AG
Samstagernstrasse 45
8832 Wollerau
Schweiz

DOLPHIN
an F24 company

T +41 44 787 30 70
F +41 44 787 30 71
info@dolphin.ch
www.dolphin.ch