MULTIFACTOR AUTHENTICATIE

HOE GOED IS DE TOEGANG TOT UW GEGEVENS BEVEILIGD?

Skyliner

ICT is mensenwerk

HOE GOED IS DE TOEGANG TOT UW GEGEVENS BEVEILIGD?

Vroeger was een enkel slot op uw deur voldoende, maar tegenwoordig is een driepuntssluiting verstandiger als u uw bedrijf wilt afschermen voor ongewenste bezoekers.

Ditzelfde geldt ook voor uw data. Het is anno nu belangrijk om de toegang tot uw 'digitale bedrijf' van een extra beveiligingslaag te voorzien.

Enkel een wachtwoord is niet meer afdoende. Deze beveiligingslaag creëert u met multifactor authenticatie. In dit document leggen we uit wat dit is.

HET BELANG VAN VEILIG WERKEN MET DATA

Weet u dat u verantwoordelijk bent voor de veiligheid van uw digitale gegevens én de gegevens van uw klant? Een digitale inbraak heeft net zoveel impact als een fysieke inbraak. Als de gegevens van u of van uw klant gestolen zijn heeft dat meestal grote gevolgen.

De gevolgen van zo'n inbraak komen soms pas na maanden of jaren aan het licht. Maar het kan ook dat de hackers zo goed buiten beeld zijn gebleven, dat u er helemaal niet achter komt! Dat geldt niet in het geval van ransomware. Kwaadwillenden breken dan in en gijzelen uw data. Dit brengt uw bedrijf per direct in een penibele situatie.

Veilig werken is niet alleen preventief, maar geeft ook een gerust gevoel. U gaat toch ook pas met een gerust gevoel op vakantie als u zeker weet dat uw huis goed op slot zit? Dit geldt ook voor de beveiliging van uw data. Het is pas echt fijn werken als u weet dat de beveiliging netjes op orde is.

VEEL VOORKOMENDE VEILIGHEIDSLEKKEN

Er zijn veel manieren waarop kwaadwillenden toegang kunnen krijgen tot uw digitale omgeving.
We noemen er vijf.

INLOGGEN BIJ OPENBARE NETWERKEN

Als u verbonden bent met een openbaar netwerk kunt u onbedoeld toegang geven tot de data die u via dat netwerk verstuurt.

PHISHING

Men probeert achter wachtwoorden te komen door bijvoorbeeld een email na te bouwen van uw provider, bank of overheidsinstantie. Door op een link te klikken in zo'n email komt u op een nagebouwde website terecht. Als u hier uw wachtwoord invult heeft de kwaadwillende toegang tot uw account.

VEEL VOORKOMENDE VEILIGHEIDSLEKKEN

WACHTWOORDEN OPGESLAGEN OP COMPUTER OF TELEFOON

Wachtwoorden opslaan in een tekstdocument is geen goed idee. Als u bijvoorbeeld uw telefoon verliest, kan men eenvoudig documenten lezen en misbruiken.

DEZELFDE WACHTWOORDEN GEBRUIKEN

Gebruikt u hetzelfde wachtwoord voor toegang tot verschillende accounts? Dit is gevaarlijk! Als bijvoorbeeld een webshop waar u klant bent gehackt wordt, kan de hacker de buitgemaakte wachtwoorden uitproberen op diensten als banken en overheden. In één klap heeft de hacker toegang tot al uw accounts!

TE SIMPELE WACHTWOORDEN GEBRUIKEN

Door een te eenvoudig wachtwoord te gebruiken is deze te kraken met een hackprogramma die miljoenen combinaties probeert. Dit noemen we brute force attack.

DE OPLOSSING: MULTIFACTOR AUTHENTICATIE

Multifactor Authenticatie is een manier om de toegang tot uw digitale informatie beter te beveiligen. De meest bekende manier van Multifactor Authenticatie is uw bankpas.

Met alleen het bankpasje kunt u niet pinnen. U heeft ook een code nodig. Maar alleen de code (zonder bankpas) geeft ook geen toegang tot uw geld. Oftewel, er zijn twee factoren nodig om toegang te krijgen tot uw geld. Namelijk de code die u onthouden hebt en het pasje dat u bij u draagt.

Multifactor Authenticatie kan op deze manier uit 3 factoren bestaan:

	**Wat u weet**	(bijv. uw pincode)
	**Wat u hebt**	(bijv. uw bankpas)
	**Wie u bent**	(bijv. uw vingerafdruk)

Als u 2 van de 3 factoren gebruikt om uw gegevens te beveiligen, zal het voor een kwaadwillende een stuk ingewikkelder zijn om digitaal in te breken.

SIMPEL EN SNEL WERKEN MET MULTIFACTOR AUTHENTICATIE IN DE PRAKTIJK

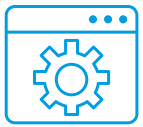
In de praktijk werkt het simpel. Wilt u op afstand inloggen in uw bedrijfsomgeving met Multifactor Authenticatie als extra beveiligingslaag? Dan vult u drie velden in.

Namelijk uw gebruikersnaam, uw wachtwoord én een extra code. Deze code wordt gegenereerd door iets wat u heeft. Bijvoorbeeld een app op uw telefoon of een speciale token die de code genereert. Deze code is tijdgebonden en wijzigt elke halve minuut.

Als een hacker onverhoopt uw wachtwoord weet te bemachtigen zal hij alsnog niet kunnen inloggen. Want hij kan de code van uw telefoon of pasje niet genereren.

UW SYSTEEM OOK BEVEILIGEN MET MULTIFACTOR AUTHENTICATIE?

Het is heel eenvoudig om te starten met Multifactor Authenticatie.



STAP 1

We installeren of activeren de software die Multifactor Authenticatie mogelijk maakt.

STAP 2

We activeren een app op de mobiele telefoons van de medewerkers of we geven hardware uit aan de medewerkers. Dit kunnen pasjes of tokens (soort sleutelhangers) zijn. Beiden hebben een klein schermpje waarop codes af te lezen zijn.

STAP 3

Met een korte workshop leggen we de werking uit aan medewerkers.

STAP 4

Uw bedrijf is nog beter beschermd tegen kwaadwillenden!

BINNEN ENKELE DAGEN GEREGELD

Wist u dat het installeren van Multifactor Authenticatie al binnen enkele dagen geregeld kan zijn?

Bel ons voor een afspraak en onze specialisten zorgen dat u snel beter beveiligd bent.

U kunt weer met een gerust hart verder werken aan uw bedrijf!

ADRES:
Skyliner
Standaardruiter 11
3905 PT Veenendaal

TELEFOON:
0318 49 50 50 (Algemeen)
0318 49 50 55 (Servicedesk)

E-MAIL:
info@skyliner.nl

WEBSITE:
www.skyliner.nl