White paper

Veiligheid

Wachtwoorden zijn achterhaald

Wachtwoorden zijn bedacht om de veiligheid te garanderen, maar de realiteit heeft deze gedachte inmiddels ruimschoots ingehaald. Toch gebruikt het gros van de bedrijven nog steeds alleen een inlognaam en wachtwoord. Hoe garandeer je dan wel veilig digitaal toegangsbeheer?

MICRO FOCUS

"Het aparte is dat bedrijven vaak heel veel geld besteden aan de fysieke toegang. Een mooie, goed beveiligde entree, camerabewaking en state of the art toegangspoortjes, maar digitaal staan er heel veel deuren op een kier."

BOUDEWIJN VAN LITH
Beveiligingsdeskundige
Micro Focus

Je hebt een inlognaam en wachtwoord voor je computer, Facebook, LinkedIn, e-mail, werkmail, energiebedrijf, bank, DigiD, webwinkels en ga zo nog maar even door. En wie heeft er voor al deze diensten nou een uniek en sterk wachtwoord met cijfers en tekens? Dat is voor de meesten veel te veel gedoe en bovendien onmogelijk om te onthouden.

Wachtwoorden veroorzaken gros van datalekken

Veel mensen gebruiken één of een aantal dezelfde wachtwoorden. Dat is natuurlijk af te raden, want als het wachtwoord gekraakt wordt, heeft de dief de sleutel in handen voor alle accounts. Cybercriminelen maken volgens onderzoek in 81% van hun geslaagde inbraken gebruik van gestolen of gemakkelijk te achterhalen wachtwoorden.

Sterkere wachtwoorden vaak geen verbetering

Het is nou eenmaal een feit: we kiezen een wachtwoord dat gemakkelijk te onthouden is. De naam van een kind, hond, de bekende cijferreeks 12345 of het moeilijker te kraken 12345678. Al jaren lang staan deze in de top 10 van populairste wachtwoorden. Systemen eisen steeds vaker sterke wachtwoorden met op zijn minst 8 karakters, een hoofdletter en een teken. De extra moeite ten spijt; Wachtwoorden worden daar niet echt veiliger op en zijn nog steeds te kraken.

Tijd voor echte veiligheid: multi-factor authenticatie

Beveiligingsexperts en technologiebedrijven zijn het er over eens: we moeten af van wachtwoorden. In oktober 2018 haalde dit bericht het NOS-journaal. Dat wachtwoorden passé zijn is eigenlijk al lang geen *breaking news* meer. Toch worden ze vooral bij bedrijven nog steeds op grote schaal gebruikt. Dus is het hoog tijd voor een veilig alternatief: multi-factor authenticatie. Dit combineert iets wat je weet (bijvoorbeeld een pincode) met iets dat je hebt (bijvoorbeeld een extra sleutel in de vorm van een usb-stick of een dynamische code via je smartphone) met iets dat je bent (bijvoorbeeld een vingerafdruk of irisscan).

Betere beveiliging; Niet alleen voor thuiswerkers

Vaak is extra beveiliging alleen weggelegd voor medewerkers die thuis mogen werken. Thuiswerkers krijgen een token of USB-stick mee die een pincode genereert om buiten de veilige muren van het bedrijf in te loggen. In een ideale situatie zou dit voor iedereen beschikbaar zijn, maar voor de meeste organisaties is dat een te grote operatie waar ze financieel en organisatorisch tegenop zien.

Digitale achterdeuren op een kier

Er zijn ook bedrijven die helemaal niets of alleen de “belangrijke” afdeling beveiligen. Denk hierbij aan de financiële afdeling. Vaak wordt verzuimd om Janice van de receptie ook van goede beveiligde toegang te voorzien. Zij logt dagelijks in met haar in de browser opgeslagen wachtwoord. Natuurlijk vormt zij een lager risico, maar als een cybercrimineel haar hackt, heeft hij zijn ingang in het bedrijfsnetwerk en kan hij vandaaruit verder. Typerend is dat bedrijven vaak heel veel geld besteden aan het beveiligen van de fysieke toegang, maar de deuren digitaal op een kier laten staan.

Een lappendeken van oplossingen

Organisaties hebben voor verschillende doelgroepen vaste soorten authenticatie; de financiële afdeling heeft usb-sleutels en de buitendienst gebruikt hun smartphone. Die verschillen zijn ontstaan omdat er door de jaren heen steeds andere eisen werden gesteld en deze eisen ook per afdeling verschilden. Deze lappendeken van verschillende oplossingen is lastig te beheren en biedt daarnaast niet de persoonlijke flexibiliteit en keuzevrijheid die je als bedrijf zou willen bieden.

Een enorme hoeveelheid accounts…

Bedrijven hebben niet alleen te maken met hun eigen medewerkers. Ze werken ook samen met ketenpartners die veilig willen inloggen om te helpen met zorgverlening, research and development, consulting of andere (tijdelijke) klussen. Daarnaast moeten ook klanten kunnen inloggen om veilig hun bestellingen te kunnen doen. Door de komst van wet- en regelgeving zoals de AVG zijn bedrijven grootschalig begonnen om hun beveiliging te verbeteren, maar ze zijn er nog zeker niet. Zo is zelfs vaak een wachtwoordbeleid niet eens ingesteld.

…en veel systemen lijken lastig te beveiligen

Beveiliging zou gemakkelijk te regelen zijn als alle doelgroepen via hetzelfde platform zouden inloggen. Dat is alleen niet het geval. Klanten loggen in op een portaal, medewerkers loggen in op het netwerk, en alle applicaties die ze gebruiken staan ook weer achter wachtwoorden. Bij web-systemen en bedrijfssystemen met 200 bedrijfsapplicaties is het niet eenvoudig om van die wachtwoorden af te komen. En om het nog ingewikkelder te maken, wil je vrijheid van inlogprocedure zodat iedereen op zijn favoriete manier kan inloggen. Rol je one size fits all uit op een grote groep medewerkers, dan is de kans groot dat sommigen moeite hebben om in de systemen te komen.

De noodzaak van verschillende inlogmethodes

Het komt regelmatig voor dat men zich in een gebied of gebouw bevindt waar geen bereik is. SMS-authenticatie zou dan niet werken. Daarnaast levert het lezen vanaf een telefoonschermpje ook regelmatig problemen op. Was het nou een kleine letter L (l), een hoofdletter i een I) een nul(0) of toch een o(o)? Ook vinden sommigen de huidige vingerafdrukscanners nog niet veilig genoeg. Je zult daarom altijd op zijn minst één alternatieve inlogmethode moeten kunnen bieden vanuit inclusiviteit.

Vrijheid voor iedereen

Voor alle gebruikers moet het risiconiveau bepaald worden en de bijbehorende inlogoptie gekozen worden. De één zal een soft token op zijn telefoon krijgen en de andere een usb-sleutel. Externe medewerkers wil je het zo gemakkelijk mogelijk maken via Out-of-band authentication. Wanneer iemand inlogt via zijn pc, krijgt hij een bericht op zijn telefoon waar alleen op 'ja' of 'nee' geklikt hoeft te worden.

Kleine fouten met grote gevolgen

Out-of-band authenticatie zou ook een goed idee zijn bij de indiensttreding van nieuwe medewerkers. Nu verstuurt IT-beheer vaak manueel een inlognaam met wachtwoord naar een privémail. Hierin schuilt een groot veiligheidsrisico. In plaats van **keesdevries@hallo.nl** krijgt **kees.de.vries@hallo.nl** de inlognaam en wachtwoord opgestuurd, soms met desastreuze gevolgen. Echter wanneer ingesteld is dat er een authenticatie via de telefoon moet plaatsvinden, is er geen vuiltje aan de lucht.

Einde aan stapelen van toegangsrechten

Geautomatiseerd autorisatie toekennen op basis van functie of rol verkleint het gevaar van het stapelen van toegang. Een junior mag in zijn eerste jaren bij een klein gedeelte van het netwerk. Enkele jaren en functies later kan hij overal bij. Bij elke functie horen meer rechten, maar oude rechten worden vaak niet ingetrokken. Met rol en functie gebaseerde toegang, en door leidinggevenden periodiek controles te laten uitvoeren, voorkom je gestapelde rechten.

Of er vanuit Kazachstan werd ingelogd? Geen idee!

Het bedrijfsleven loopt qua toegangsbeheer enorm achter op de consumentenmarkt. Elke consument kent de geautomatiseerde, extra beveiligingsmaatregelen als je in het buitenland of vanaf een ander apparaat wil e-mailen of Facebooken. Vragen we in het bedrijfsleven aan IT-beheer of er dit weekend ook vanuit Kazachstan is ingelogd, dan kunnen ze dat meestal helemaal niet zien. Tegenwoordig kan dat veel beter.

Inloggen op basis van je gedrag

Moderne systemen maken gebruik van adaptive, risk based of context based authenticatie. Dit is de evolutionaire stap binnen de wereld van het inloggen. Hierbij krijg je op basis van datum, tijd, locatie of apparaat gemakkelijk toegang via een extra stap. Het systeem kijkt niet alleen waarvandaan, hoe laat en met welk apparaat je inlogt. Het kan ook een extra barrière opwerpen bij verdacht gedrag. Dat kan real-time op basis van historisch gedrag. Normaal kopieert Vanessa overdag zo'n 3 documenten van de fileserver. Ineens verwijdert ze er 20 om 3 uur 's nachts. Het afwijkend gedrag wordt gesignaleerd en haar account direct geblokkeerd.

Sleutel tot succes: beveiliging vanuit de infrastructuur

Beveiliging wil je het liefst in één keer voor iedereen regelen. Authenticatie zou een onderdeel moeten zijn van het netwerk. Een infrastructuurvoorziening waar alle systemen en applicaties gebruik van maken en elke mogelijke authenticatiemethode op aan kan haken. Van biometrie (als vingerafdruk en irisscan), tot hardware en software tokens, OTP (SMS) tot en met usb-sleutels en alles wat in de toekomst nog ontwikkeld gaat worden.

Tijd voor echte veiligheid

Wachtwoorden zijn duidelijk passé en vormen een beveiligingsrisico. Daarom is het de hoogste tijd om op een andere manier in te gaan loggen door gebruik te maken van één systeem waarop alle bestaande en nieuwe authenticatiemethoden centraal kunnen worden aangehaakt (voor zowel on-premise als cloud-systemen). Micro Focus® helpt meer dan 40.000 bedrijven wereldwijd op een veiligere manier werken. Hoe we dat doen, zie je op **www.microfocus.com**.

Contacteer ons op:
www.microfocus.com

Vind je het leuk wat je leest? Deel het.