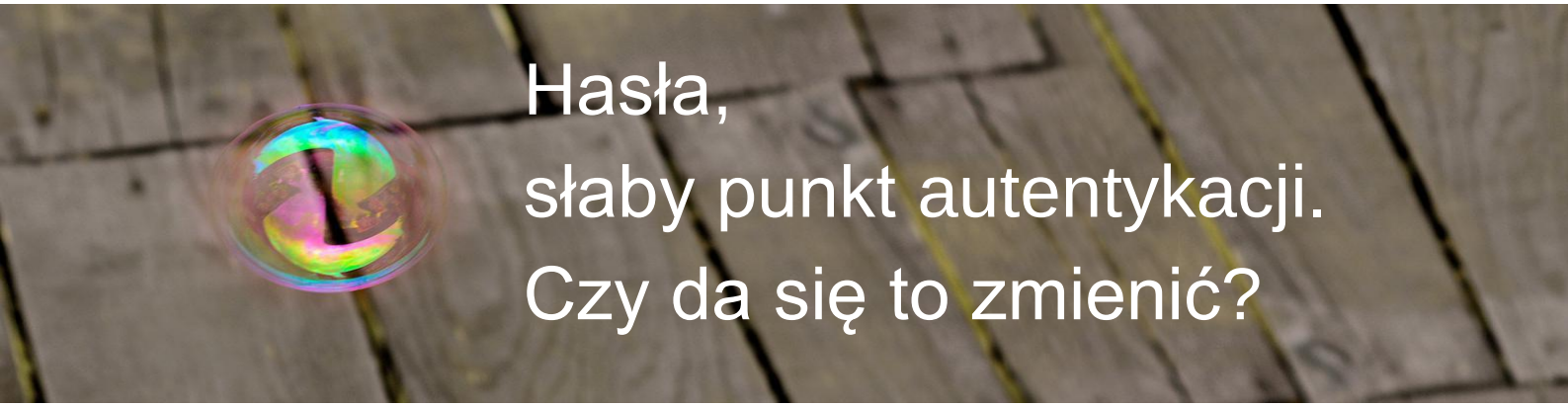
SECRET DOUBLE OCTOPUS

QDP
Efektywność i bezpieczeństwo IT



Hasła, słaby punkt autentykacji. Czy da się to zmienić?

Dlaczego hasła są słabym punktem autentykacji?

Jak na ironię jednym z najczęściej kradzionych haseł jest „password" wraz z nie mniej popularnym „123456"[1]. Średnio uzdolnionemu hakerowi nie zajmuje wiele wysiłku odgadnięcie prostego hasła, lub też odtworzenie hasła, których nie można w łatwy sposób odgadnąć. Zawsze pozostaje bowiem możliwość uzyskania użytecznych informacji poprzez atak phishingowy.

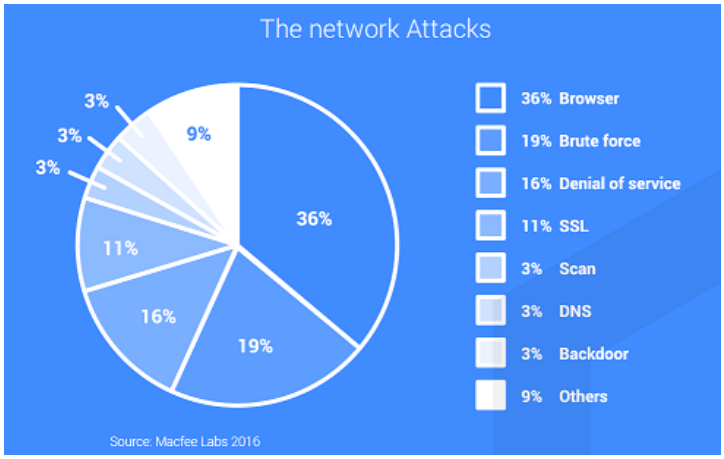
Od lat organizacje edukują pracowników w zakresie tego, jak wielkie znaczenie mają bezpieczne hasła[2] i jak skutecznie opierać się atakom phishingowym. Wysiłki te jednak zbyt często zawodzą.

Ponad połowa procent potwierdzonych naruszeń dostępu do danych wiąże się z wykorzystaniem słabych, domyślnych lub skradzionych haseł. Jednocześnie liczba ataków phishingowych i innych przeprowadzonych przy użyciu poczty elektronicznej wzrosła prawie o połowę w ostatnich latach[3].

Według NIST[4], amerykańskiego Narodowego Instytutu Standardów i Technologii, jedynym sposobem na to, aby hasła były skuteczne, jest wymaganie od użytkowników stosowania w standardowych hasłach 16 znaków, zarówno liter, jak i cyfr, z dużymi literami i/lub symbolami alfanumerycznymi) lub wręcz użycie 64 znaków, co wymagane jest przez większość organizacji.

Raport McAfee[5] wymienia siedem najpopularniejszych typów ataków sieciowych, jakie zostały zaobserwowane w niedawnym czasie. Drugim co do wielkości typem ataku (19 procent całości) były ataki Brute Force, w których haker próbuje rozszyfrować hasło lub numer PIN metodą prób i błędów.

Jeśli spojrzymy na poprzednie lata, zauważymy ogromny wzrost liczby przypadków włamań do kont użytkowników. Zgodnie z raportami ITRC Data Breach Reports [6] na ujawnienie narażone zostało ponad 170 milionów rekordów danych osobistych przechowywanych przez instytucje finansowe, edukacyjne, instytucje ochrony zdrowia i medyczne, przedsiębiorstwa, wojsko oraz rząd.
Tylko w jednym badanym roku dane te zostały ujawnione w blisko 780 przypadkach dokonanych naruszeń.



1 Announcing our Worst Passwords of 2016, TeamsID, March 30, 2017
2 Data Breach Investigations Report, Verison, 2016
3 BEC attacks up 45% and gaining in sophistication: Proofpoint, SC Media, March 23, 2017
4 NIST Special Publication 800-63B Digital Identity Guidelines
5 Threats Report, McAfee Labs, March 2016
6 Data Breach Reports, Identity Theft Resource Center, 2016 EOY Report
7 No password, phone sign in for Microsoft accounts, Microsoft, April 18, 2017

Czy jest inne rozwiązanie?

Jedną z możliwości uniknięcia nieuprawnionego dostępu do danych, jest logowanie poprzez autentykację typu ‘push’ z wykorzystaniem urządzenia mobilnego. Mechanizm ten został zaimplementowany m.in. przez firmę Microsoft[7]. Użytkownicy w trakcie logowania zamiast wpisywać hasło, które może zostać zapomniane, wyłudzone lub też złamane, mogą skorzystać z możliwości otrzymania powiadomienia typu ’push’.

Jak działa ‘push’?

Użytkownik otrzymuje kod weryfikacyjny i zatwierdza otrzymane powiadomienia w aplikacji. Logowanie nie wymaga podawania hasła, a cała weryfikacja tożsamości odbywa się w telefonie.
Proces ten funkcjonuje jak weryfikacja dwuetapowa, która wymaga czegoś, co wiesz (PIN telefonu lub parametry biometryczne) i czegoś co masz (telefon).

Dlaczego logowanie z wykorzystaniem telefonu jest bezpieczniejsze, niż wpisywanie hasła?

Obecnie większość osób loguje się do stron internetowych lub aplikacji za pomocą nazwy użytkownika i hasła. Niestety hasła mogą zostać zapominane, skradzione lub odgadnięte. Aplikacja do logowania bez hasła generuje widoczny na telefonie klucz, który odblokowuje konto użytkownika. Klucz ten jest chroniony kodem PIN lub parametrami biometrycznymi użytkownika telefonu. W trakcie logowania za pomocą telefonu, klucz wykorzystywany jest do bezpiecznego potwierdzenia tożsamości za pomocą dwóch czynników - samego telefonu i możliwości jego odblokowania przez użytkownika.

Dla środowisk bez haseł wymagana jest silna autentykacja.

Moduł uwierzytelniający Octopus Authenticator wykorzystuje mechanizm ‘secret sharing’ do ochrony dostępu do składowanego hasła poprzez wiele kanałów. Ujawnienie pojedynczej informacji nie powoduje zagrożenia dla bezpieczeństwa, gdyż platforma jest na to odporna. Octopus jest pierwszą kompleksową platformą zastępowania haseł, wykorzystującą wieloskładnikowe mechanizmy zabezpieczeń oraz algorytmy sklasyfikowane przez teorię informatyki jako niemożliwe do złamania.

Silna autentykacja	**Pełna ochrona**	**Otwarta platforma**
aplikacje mogą niezawodnie wykorzystać smartfon jako podstawowy czynnik uwierzytelniania	cyklu życia tożsamości użytkownika, począwszy od rejestracji, po jej odwołanie	obsługuje wiele mechanizmów autentykacji: SAML, Radius, OpenID, FIDO, Active Directory i inne

Secret Double Octopus opracowała jedyną na świecie technologię bezkluczowego uwierzytelniania wielowarstwowego, zapewniającą ochronę tożsamości i danych w środowiskach chmurowych, mobilnych i IoT. W oparciu o algorytmy Secret Sharing, pierwotnie opracowane w celu ochrony kodów startowych broni jądrowej, technologia Secret Double Octopus chroni dostęp do krytycznych informacji przed atakami cyberprzestępców, eliminując tym samym zagrożenia takie, jak ataki brute force, Man-In-The-Middle, manipulacje PKI, kradzież klucza czy luki bezpieczeństwa urzędów certyfikacji.

Przedstawicielem Secret Double Octopus w Polsce jest QDP Sp. z o.o.

SECRET DOUBLE OCTOPUS

www.doubleoctopus.com

www.qdp.com.pl

QDP Sp. z o.o.
ul. Ślężna 104, 53-111 Wrocław
tel. 71 356 49 40
info@qdp.com.pl

Centrum Kompetencyjne
ul. Nabielaka 6, 00-743 Warszawa
tel. 22 160 51 77
www.qdp.com.pl

QDP