Microsoft oficjalnie: nie powinno się wymuszać okresowej zmiany haseł! Zmiany w Windows 10 i 2016 server

03 CZERWCA 2019, 21:28 | W BIEGU | KOMENTARZY 21

TAGI: HASŁA, MICROSOFT, WINDOWS

W Rekomendowanych ustawieniach dotyczących bezpieczeństwa Windows 10 i Windows Server 2016: „Security baseline (FINAL) for Windows 10 v1903 and Windows Server v1903” Microsoft napisał tak:

> ***Dropping the password-expiration policies that require periodic password changes.***

Dalej czytamy wyjaśnienie:

> *When humans pick their own passwords, too often they are easy to guess or predict. When humans are assigned or forced to create passwords that are hard to remember, too often they'll write them down where others can see them. When humans are forced to change their passwords, too often they'll make a small and predictable alteration to their existing passwords, and/or forget their new passwords. When passwords or their corresponding hashes are stolen, it can be difficult at best to detect or restrict their unauthorized use.*
>
> *Recent scientific research calls into question the value of many long-standing password-security practices such as password expiration policies, and points instead to better alternatives such as enforcing banned-password lists (a great example being Azure AD password protection) and multi-factor authentication.*

Czyli w wolnym tłumaczeniu – wymuszenie haseł daje więcej złego niż dobrego. I być może lepiej uniemożliwić używania złych haseł (np. zbyt prostych, wyciekłych) czy postawić na wieloczynnikowe uwierzytelnienie.

–ms

Spodobał Ci się wpis? Podziel się nim ze znajomymi:

INFO O SEKURAK HACKING PARTY

Email *

Z jakiego miasta jesteś?

Zapisanych: 2558. Tu otrzymasz info o obecnych / planowanych Sekurak Hacking

Party.
Okazjonalnie również ogólne info od załogi Sekuraka.

Zapisuję się!

Komentarze

w666
3 czerwca, 2019 | 9:55 pm

Po co wymuszać na ludziach używanie trudnych haseł, jeśli są debilami i są nadal gotowi ustawiać sobie abc123, to niech sobie ustawiają, to jest i będzie ich problem.

Odpowiedz

jmper
4 czerwca, 2019 | 5:40 am

Otóż nie, nie jest to i nie będzie tylko ich problem. W przypadku organizacji jest i będzie to również problem organizacji, ponieważ to dane tej organizacji wyciekną w wyniku złamania hasła, oraz to do tej organizacji włamią się przestępcy wykorzystując słaby punkt którym jest zbyt proste hasło.
W przypadku takiego np. banku, jeśli hasło użytkownika zostanie złamane i wyjdzie na jaw że bank nie forsował konieczności używania silnych haseł, to po pierwsze taki bank będzie musiał klientowi zwrócić skradzione pieniądze, po drugie zostanie ukarany przez odpowiednie organy nadzoru za nieprzestrzeganie dobrych praktyk. Zatem czasem warto zdjąć klapki z oczu i spojrzeć nieco dalej niż czubek własnego nosa, choć rozumiem przyjemność jaką daje łatwe osądzenie bliźnich i w tym kontekście wykazanie swojej własnej zajebistości.

Odpowiedz

NEWSY NA EMAIL

Podaj swój adres e-mail. Informacje o postach prześlemy automatycznie.

OK!

ARTYKUŁ TYGODNIA

Jak zdroworozsądkowo podejść do analizy ryzyka IT?

FACEBOOK

W BIEGU

Arturo

4 czerwca, 2019 | 7:12 am

Spójrz na temat szerzej…

Jeśli ktoś używa prostego hasła na komputerze przenośnym, który jest jednocześnie sprzętem korporacyjnym i komputer zostanie takiej osobie skradziony, dla przykładu niech to będzie manager średniego szczebla, a przechowywał na nim choćby personalia klientów organizacji, to nie jest to wyłącznie jego problem. W przypadku złamania tego hasła i wycieku tych danych winę poniesie również firma…

Odpowiedz

KW

4 czerwca, 2019 | 7:40 am

Do czasu kiedy ktoś ustawi sobie proste hasło na bazę z np. twoimi danymi osobowymi. Wtedy to nie będzie tylko ich problem.

Odpowiedz

Szymon

4 czerwca, 2019 | 8:18 am

Chyba, że pracują w Twojej firmie i mają dostęp do danych, których nie chcesz udostępniać całemu światu.

Odpowiedz

xor

4 czerwca, 2019 | 9:01 am

Colonial Pipeline dotknięty ransomware. Zamknęli rurociąg transportujący 45% paliw konsumowanych na wschodnim wybrzeżu USA!

Jedna z najbogatszych gmin w Polsce – po raz drugi zaatakowana przez ~hackerów. W tle 5 milionów złotych

Masowe odłączenia prądu w Polsce. A, nie czekaj – to SMSowe oszustwo

Jaka jest najczęstsza zła rada udzielana w kontekście haseł?

Możliwość wykonania dowolnego kodu w popularnej bibliotece ExifTool. Exploitem może być ~najzwyklejszy plik .jpg

Jak ktoś zacznie Ci puszczać tony spamu przez serwer pocztowy to zrozumiesz. Widać, że nie jesteś adminem.

Odpowiedz

Monter
4 czerwca, 2019 | 6:38 pm

Rozumiem, że do Twojego serwera poczty, do którego logują się zwykle np. pracownicy biura w PL w określonych godzinach oraz wysyłający niewielkie ilości e-maili nagle z drugiego końca świata może się ktoś w nocy uwierzytelnić i wysłać na raz kilka pierdylionów przesyłek?

Odpowiedz

John Sharkrat
5 czerwca, 2019 | 2:36 pm

To nie jest ich problem, tylko organizacji w której pracują.

Odpowiedz

Tomasz21.
4 czerwca, 2019 | 1:10 am

Witam; W pełni się zgadzam z @w666. Dla tych lekko ograniczonych, to chyba nic nie może pomóc. To człowiek, jest podobno istotą rozumną; Więc niech korzysta z tego udogodnienia. To przecież człowiek decyduje, co się dzieje na jego Pc-cie. Przecież Sekurak cały czas wałkuje te tematy. Wystarczy poczytać wpisy, jakie tutaj można znaleźć. Ja wiem że ta sprawa dotyczy innej klienteli. Ale przecież oni też mogą tutaj zaglądnąć i się troszkę pod-uczyć. Wystarczy, trochę dobrych chęci. Pozdrawi

Odpowiedz

POLECAMY

Wymogi audytu bezpieczeństwa w jednostkach administracji publicznej

Bezpieczeństwo WiFi: 9-częściowy kurs

OSTATNIE KOMENTARZE

Tomasz o Jedna z najbogatszych gmin w Polsce – po raz drugi zaatakowana przez ~hackerów. W tle 5 milionów złotych

Piotr o Jaka jest najczęstsza zła rada udzielana w kontekście haseł?

GallAnonim o Jaka jest najczęstsza zła rada udzielana w kontekście haseł?

jan o Z jakich Twoich danych może korzystać Whatsapp/Messenger/iMessage/Signal/Telegram?

GallAnonim o Jaka jest najczęstsza zła rada udzielana w kontekście haseł?

sasza o Jedna z najbogatszych gmin w Polsce – po raz drugi zaatakowana przez ~hackerów. W tle 5 milionów złotych

sasza o Colonial Pipeline dotknięty ransomware. Zamknęli rurociąg transportujący 45% paliw

~kn
4 czerwca, 2019 | 6:20 am

W środowiskach służbowych w pierwszej kolejności będzie to problem pracodawcy lub kontrahentów.

Odpowiedz

Piotr
4 czerwca, 2019 | 6:26 am

Ale to już dawno mówiłem, jeszcze za czasów AD na bazie W2000. Każdy wtedy kazał pukać mi się w głowę.

Odpowiedz

John
4 czerwca, 2019 | 8:50 am

Wymuszanie zmiany haseł ma sens tylko wtedy, jeśli w organizacji zmieniły się zasady dotyczące jego złożoności (liczba znaków, znaki specjalne, zabronione znaki). W innym przypadku mija się z celem.

Odpowiedz

Vim
4 czerwca, 2019 | 2:56 pm

są różne sytuacje, po (potencjalnym) wycieku lub naruszeniu bezpieczeństwa czy innej potencjalnie zagrażającej sytuacji warto wymusić na użytkownikach zmianę. W normalnym funkcjonowaniu codziennym zgadzam się z MS, że nie warto. Zmiana polityki

konsumowanych na wschodnim wybrzeżu USA!

PierwszY o Jedna z najbogatszych gmin w Polsce – po raz drugi zaatakowana przez ~hackerów. W tle 5 milionów złotych

Tosiek o Jedna z najbogatszych gmin w Polsce – po raz drugi zaatakowana przez ~hackerów. W tle 5 milionów złotych

7mln o Jedna z najbogatszych gmin w Polsce – po raz drugi zaatakowana przez ~hackerów. W tle 5 milionów złotych

TEMATY

android anonimowość Apple atak backdoor bezpieczeństwo bug bounty ciekawostki Exploit Facebook firefox google hack hacking hasła Internet iOS iot iphone książka linux malware Microsoft nsa oszustwo patronat Phishing podatności podatność prywatność ransomware rce rodo root sekurak shp szkolenie szyfrowanie vulnz websecurity wifi Windows wyciek XSS zabezpieczenia

dotyczącej haseł nie następuje raczej tak często, ale zgodzę się ,że również warto wymusić zmianę w takiej sytuacji

Odpowiedz

Luke

4 czerwca, 2019 | 5:52 pm

Drogi Xor'rze tak sie sklada, ze to nie admin jest klientem. Klientowi ma byc latwo, wygodnie i przejrzyscie, a przede wszystkim ma mu sie nie zawracac tak zwanej dupy.

Admin natomiast jest pracownikiem i ma robic co mu kaza, a nie plakac, ze musi wykonywac prace administracyjne. Dodam, ze mowie to z perspektywy developera. Klient placi klient wymaga.

Odpowiedz

Wredny

6 czerwca, 2019 | 12:34 pm

Skoro (cyt.) „a klient (użytkownik) ma to w nosie – chce i ma pracować bez przeszkód.", to co stoi na przeszkodzie, żeby w firmie takich delikwentów zatrudnić na stanowiskach gdzie haseł się nie wymaga?! Ot, choćby na stanowiskach konserwatorów powierzchni płaskich! Jak użyszkodnik chce mieć komputer na biurku i do tego ze swobodnym dostępem do internetu, to niech stosuje się do zaleceń płacących za siedzenie za biurkiem! A jak nie, to przyjdzie ktoś inny! I gdyby takie podejście funkcjonowało także w urzędach, to jako podatnicy nie płacilibyśmy za koncert życzeń urzędników, którego realizacja i tak nic nie zmienia od lat! Jak w urzędach pojawiły się komputery, to kolejki w okienku wydłużyły się znacząco! I co zabawniejsze, im wydajniejsze windowsy, tyk kolejki dłuższe! No to gdzie leży problem szanowni gadżeciarze zajmujący stanowiska informatyków w urzędach i firmach?!

Odpowiedz

mft555
5 czerwca, 2019 | 9:37 am

Śmiesznie to brzmi jak używają słowa humans a nie people.

Odpowiedz

HansKiełbasa
5 czerwca, 2019 | 8:11 pm

Jeszcze niech PTH i PTT dla kont domenowych uniemożliwią i ok.

Odpowiedz

sK!
6 czerwca, 2019 | 8:45 am

Zgadzam się z Lukiem, Admin podnieca się technologiami i tym co może skonfigurować na swoim serwerze, a klient (użytkownik) ma to w nosie – chce i ma pracować bez przeszkód. W niektórych firmach mam tak upierdliwych i nieżyciowych IODów, że aż przykro, bo zmiana haseł w AD pociąga za sobą masę konsekwencji w urządzeniach nie LDAPowych. I tak po 30 dniach użytkownik nagle nie może zrobić skanu, albo dogadać się z jakimś innym aparatem. Nie wiem czy zwróciliście uwagę, że w przytoczonym cytacie MS ot tak sobie wtrąca „(a great example being Azure AD password protection”. Czyli mamy sprzedawać chmurę i koniec i mam wrażenie, że głównie o to chodzi.

Odpowiedz

qlawy

6 czerwca, 2019 | 11:26 am

Ujmę to tak:

through 20 years of effort, we've successfully trained everyone to use password that are hard for humans to remember, but easy for computers to guess.

Hasła muszą być zmieniane – jest to element bezpieczeństwa – coś co wiem. Nie istotne jest na co – łatwe, trudne – ważne, aby regularnie zmieniać.

Odpowiedz

Alf/red/

7 czerwca, 2019 | 10:59 am

Ale cały artykuł jest polemiką z „ważne, aby regularnie zmieniać". Tymczasem Ty przy swoim, bez żadnego argumentu. Ale dlaczego ważne? Przed czym broni? Czy nie mamy innych metod i sposobów, żeby przed tym bronić równie dobrze?

Odpowiedz

sdfdfgggggd

10 czerwca, 2019 | 1:30 pm

Raz na ileś warto. Zdobywając cudze hasło nie trzeba robić od razu demolki. O wiele więcej można osiągnąć podszywając się pod właściciela przez długi, dłuuugi czas tak, żeby on się nie skapnął.

Odpowiedz

Odpowiedz

Imię *

Mail (Nie zostanie opublikowany) *

WWW

Wyślij komentarz

Nota prawna