公司該怎麼制訂密碼變更政策？

微軟日前宣佈取消預設密碼最大使用期限（maximum password age）的政策再度引發強迫密碼變更的爭辯。本文將說明企業仍應持續密碼效期設定的理由。

文／Roger A. Grimes譯／葉庭筠

微軟在今年4月24日宣佈移除Windows「密碼最大使用期限」（Maximum Password Age），即強迫密碼到期的預設規則。Windows預設（及建議）的最長密碼效期為45到60天，視作業系統版本而定。

微軟是在最近美國國家標準與技術研究院（National Institute of Standards and Technology, NIST）建議除非發現密碼被破解，否則無需變更密碼後，宣佈移除強迫到期的預設規則。

微軟的理由是，密碼通常是經由密碼猜測／暴力破解以外的方式被攻破，後者正式密碼強迫到期試圖解決的問題。此外，微軟覺得強迫用戶變更密碼往往反而會使他們把同一組密碼或模式重覆用於多個網站。密碼大部份是被網釣攻擊竊走，強迫變更密碼根本無助於防止。

那麼，你是否應以NIST和微軟馬首是瞻，取消強迫密碼到期的政策？我認為萬萬不可，理由如下。

法規仍然要求設定密碼到期

我還沒碰到完全不需遵循網路安全規定或法規（如PCI-DSS、HIPAA、SOX、NERC）的公司單位。所有這些規定都要求定期自動變更密碼。如果你聽從NIST新的密碼建議，那麼祝你好運。除非這些規定全都修改掉，否則你會被一堆現有建議卡死。

密碼被破解時很難發現

我對「除非你發現密碼被破解否則不要變更密碼」最大的疑問是大部份人根本無從知道密碼是否被破解了。根據我看過的所有「停留時間」（dwell time）資料，駭客取得網路及密碼完整存取權限之後要好幾個月受害者才會發現這件事。

暗網或pastebin網站（***譯註：原始碼儲存分享始祖***）上流傳的數億筆密碼中，許多都是好多年前就被破解的，其中還有不少現在都還可以用，因為用戶一直沒改過。光是這點就足以證明強迫變更密碼的必要性。

強迫用戶定期更新密碼就可以降低被盜密碼的攻擊事件，或是整批被公佈於網上的風險。這也是推動密碼自動到期的第二大理由，僅次於法規遵循。

強迫更新並不會拉高密碼重覆使用率

前面提及，強迫變更密碼被認為會造成用戶重覆使用同一組密碼或相同模式於多個不同網站上。但我從NIST的任何資料都看不到這點。或許真的有這類資料，但我找了好多年都沒找到。

網站定期要求你變更密碼時，很少人會乖乖變更每個網站的每組密碼。真實情況是使用者有的網站會改，有的不會改，在公司網站尤其如此。當某個網站（或單位）比其他網站更常要求變更密碼時，通常結果是讓它的密碼獨一無二，或

是使和它共用密碼的網站變少。反之，長年不要求變更密碼的網站會讓它更容易和別的網站共用一組密碼。

NIST還推測，複雜密碼會讓用者更容易重覆用於多個網站上。不過我也沒看到支持該論點的資料，我甚至覺得不太可能。如果你喜歡設定長或複雜密碼，你會發現不同網站對長或複雜的定義都不同。有的網站接受8到12碼，有的網站不接受英文字母以外的符號。另一些網站只允許數字和字母。你想把同一組複雜的長密碼套用在不同網站，若都行得通也算你幸運。

密碼猜測及暴力破解依然存在

即使今天密碼猜測和暴力破解不像以前那麼流行，但還是存在，每年仍然造成數萬起帳號被駭事件。有一大堆惡意程式可以猜測個人或企業密碼，每天無時無刻都有機器人試圖突破微軟遠端桌面協定（Remote Desktop Protocol, RDP）、Putty、VNC、SSH和入口站登入機制。使用複雜的長密碼就可以阻擋掉這些攻擊，但往往受害者就是不願這麼做。採取強迫變更密碼手段，惡意軟體或駭客就只能有更少時間來猜測或暴力破解密碼，不論密碼長度或複雜性。

只要密碼猜測或破解手法存在一天，能減少風險的任何事都值得。若想要我改變立場，唯一方法是證明強迫變更密碼會提高風險。我至今沒有看到這種資料，反而看到上萬人密碼遭到機器人程式破解。

我能透過電子郵件竊取你的密碼

我可以在電子郵件中加入一則嵌入式連結，只要你點擊它，就可以讓你的瀏覽器把Windows密碼雜湊值傳給我。防範方法是有的，但大部份公司都未實作正確的防護，特別是經常有行動裝置用戶離開公司網路的企業。

這個做法中，瀏覽器並不會把你的密碼以明碼傳送給我，而是送給我Windows NTLM 挑戰回應交握（challenge-response handshake）（***譯註：Windows NTLM為一種Windows系統的網路驗證協定***），許多駭客工具可以從中抓出密碼雜湊值。你的密碼雜湊值可以用在其他攻擊上，也可以用來破解你自己的明碼密碼。

8位密碼雜湊對駭客來說基本上是小兒科，不論它有多複雜。我曾看過不少次12位密碼雜湊被破解，還看過幾次16位密碼被破的。它們都不是極端複雜，但大概反映了大部份環境的密碼樣貌。只要駭客能誘騙你點入郵件中的嵌入連結，取得你的密碼雜湊值，不定期變更密碼就會招致更大風險。

你該多久變更一次密碼？

微軟官方並未建議說密碼可以永久不過期，他們是交由企業管理員決定。這就是一門學問了。

如果你必須遵循要求密碼自動失效的法規，那這點就是假議題了；法規怎麼要求你就得怎麼做。如果你可以決定公司的密碼最大使用期限，就取決於貴公司的風險容忍度。我認為每30到45天強迫變更一次是太誇張了，間隔那麼短，員工真的就會重覆使用密碼。一般企業可能每90天變更一次，我覺得（因為我沒有任何實際資料支持），如果企業希望風險遠比其他人低，90天差不多。我覺得謹慎度一般的企業會拉長到180天到365天才要求變更一次。

若管理員完全不強迫密碼到期，可以說是為駭客或惡意程式入侵開了方便之門，至少在有人拿出資料反駁我之前，我是這麼覺得。