Прилагайте политика за използване на силни пароли!

Атаките срещу пароли могат да бъдат от различно естество: атаки от типа на “Brute Force” (нападателят опитва възможно най-много комбинации) или чрез речници (нападателят опитва най-често срещаните пароли, които той притежава, дали общи имена или опростени комбинации като „azerty“). Атаките могат да бъдат и от типа „социално инженерство“: нападателят тества лична информация като имената на вашите роднини или прякорите на вашите домашни любимци, която е събрана от социалните мрежи. Тези атаки могат да бъдат извършени и чрез елементи, които вече са налични онлайн, без ваше знание, например база данни, лошо защитена от доставчик, в която фигурират вашите идентификатори за дадена услуга. Атака срещу паролите може да няма за цел да бъде ограничена до засегнатата услуга, но да позволява разпространение на атаката в компанията или към нейните партньори. Например, вашият имейл може да бъде използван от нападателя за изпращане на фишинг и спам съобщения до вашите професионални контакти, за да ги насърчите да предприемат действия като щракване върху връзка към уебсайт - т.нар. фишинг.

Експертите препоръчват дължината на паролата да бъде свързана с критичността на услугата, до която дава достъп, с минимум 9 знака за некритични услуги и минимум 15 знака за критични услуги. Силната парола съдържа главни и малки букви, числа и специални знаци. Паролите не трябва да съдържат никакви лични елементи - дата на раждане или собствено име. Възможно е да използвате думи - паролите ще се състоят от произволно избиране на определен брой думи от даден корпус, напр. речник. За всяка изисквана услуга са необходими различни пароли. Не използвайте една и съща парола за личните и служебните си акаунти. Чрез използването на мениджър за пароли съхранявате своите комплексни и

надеждни пароли и не се налага да ги запомняте. Той позволява да се запишат всички пароли в криптиран файл, достъпен само с една уникална парола. Много услуги вече позволяват да се подсили паролата чрез вторично удостоверяване. Изберете многофакторното удостоверяване – то осигурява ниво на допълнителна сигурност. Това решение се основава на два фактора: парола, но също и потвърждение чрез код, предаван чрез режим на връзка на трета страна.