Stockholm

2017-03-30

**13 orsaker till varför lösenord inte är säkra**

**Det är inte en bra idé att använda användarnamn och ett statiskt lösenord som autentiseringsmetod för inloggningar, eftersom det dramatiskt ökar risken för obehörig åtkomst till tjänster och information. Stefan Sundh, specialist på användarautentisering på identitets- och säkerhetsföretaget Nexus Group, går igenom 13 orsaker till varför lösenord inte är säkra.**

1) Användare återanvänder ofta samma lösenord för olika tjänster.

"Det här innebär att om lösenordet för en tjänst kommer i orätta händer så får obehöriga inte bara tillgång till just den tjänsten utan också till en rad andra tjänster", säger Stefan Sundh.

2) Många människor ändrar inte omedelbart standardlösenord, vilket innebär att det är lätt för obehöriga att få åtkomst.

"Standardlösenord är ofta tillgängliga för allmänheten i handböcker, och de är ofta också ganska lätt att gissa. Dessutom är det inte alls ovanligt att de offentliggörs i hackerforum", säger Stefan Sundh.

3) Lösenord delas ofta mellan användare.

"Det här innebär att organisationer inte kan vara säkra på vem som egentligen har tillgång till tjänster och information", säger Stefan Sundh.

4) Användare tenderar att behålla samma lösenord under en lång tid.

"Om en obehörig person får tag på lösenordet kan de fortsätta att använda det för obehörig åtkomst under en lika lång tid", säger Stefan Sundh.

5) Verktyg för att knäcka lösenord håller på att bli *riktigt* bra på att gissa lösenord.

"De tekniska framstegen inom det här området går riktigt snabbt – det är bara en tidsfråga innan lösenord som i dag anses starka snart kommer att kunna knäckas", säger Stefan Sundh.

6) Människor använder ofta alltför svaga lösenord.

"Det här kan även göra det möjligt för människor att gissa lösenord utan hjälp av verktyg", säger Stefan Sundh.

7) Lösenord stjäls enkelt med hjälp av social ingenjörskonst (social engineering).

"Det finns ett oändligt antal metoder, till exempel övertygande e-postmeddelanden eller falska webbplatser där människor ombeds att dela sitt användarnamn och lösenord. Och en överraskande stor andel av användare delar faktiskt med sig av sin inloggningsinformation när de ombeds göra det", säger Stefan Sundh.

8) Lösenord skickas ibland över osäkra nätverk, vilket gör dem lätta att stjäla.

"Du vet det där trådlösa nätet på ditt favoritkafé? Det är troligen ett osäkert nätverk", säger Stefan Sundh.

9) Organisationers lösenordsdatabaser blir hackade mycket oftare än de flesta tror.

"I många fall upptäcks aldrig hackerattacken av någon, eller så tar det lång tid för någon att lägga märke till vad som hänt. Det här innebär att hackarna under tiden kan använda lösenorden hur mycket som helst för att få tillgång till alla typer av känslig information", säger Stefan Sundh.

10) Användare skriver ofta ner lösenord, till exempel på klisterlappar.

"Det här gör naturligtvis lösenorden mycket lätt att stjäla", säger Stefan Sundh.

11) Lösenord kan stjälas av skadliga program utrustade med komponenter för tangentbordsloggning.

"Någon som vill åt ditt lösenord kan mycket enkelt få tag på den här typen av programvara", säger Stefan Sundh.

12) Om ett lösenord hamnar i orätta händer kan obehöriga personer få tillgång till den aktuella tjänsten och all dess information utan att någon märker det.

"Användaren har ingen aning om att någon annan har tillgång till tjänsten med användarens lösenord. Och kanske ännu värre: den organisation som tillhandahåller tjänsten vet inget heller, vilket innebär att externa personer obemärkt kan stjäla företagskänslig information", säger Stefan Sundh.

13) Organisationer missar ofta att ta bort användarkonton och tillhörande lösenord när anställda slutar sina jobb, vilket innebär att de före detta anställda fortsätter ha tillgång till information som de inte längre borde kunna komma åt.

"Det här är jättevanligt – det är helt galet, det finns inget annat sätt att uttrycka det", säger Stefan Sundh.

**Om Nexus Group**

Svenskägda Nexus Group är ett innovativt och snabbväxande produktbolag som utvecklar identitets- och säkerhetslösningar. Vår teknik hjälper organisationer att digitalisera sina verksamheter på ett säkert sätt genom att: skydda e-handel eller nätbank, hantera fysisk och digital åtkomst, säkra kommunikation mellan saker, skydda e-tjänster i offentlig sektor, ta fram inloggnings- och passerkort, samt säkra inpassering.

Att skapa, hantera och använda identiteter är själva fundamentet för all säkerhet, både fysisk och digital. Vi har gjort identiteterna pålitliga för människor, mjukvaror och saker ända sedan 1984, och vår teknik är i dag betrodd av en lång rad organisationer och 100 miljoner slutanvändare runt om i världen. Vi är 300 medarbetare på 15 kontor i Europa, Indien och USA, och har ett globalt partnernätverk.

Nexus mission är att bidra till ett säkrare samhälle, och allt vi gör styrs av våra kärnvärden: we care, we innovate, we are committed.

**Kontaktpersoner**:

Carolen Ytander, CMO på Nexus Group.

carolen.ytander@nexusgroup.com

+46 729 74 34 61

Stefan Sundh, specialist på användarautentisering på Nexus Group.

stefan.sundh@nexusgroup.com

+46 702 69 14 62

**Pressbilder:**

[Carolen Ytander](http://www.mynewsdesk.com/uk/nexus/images/carolen-ytander-01-665818)

[Stefan Sundh](https://www.mynewsdesk.com/se/nexus/images/stefan-sundh-mg-6083-640x410-819150)