Det månedlige nyhedsbrev om IT-sikkerhed til dig

Password på den simple måde

Oversigt

Du får ofte fortalt, at adgangskoder er nøglen til at beskytte dine konti (hvilket er sandt!), Men sjældent får du en enkel måde til sikkert at oprette og administrere alle dine adgangskoder. Nedenfor forklarer vi i tre enkle trin hvad du kan gøre for at forenkle dine adgangskoder, sikre dine konti og beskytte din fremtid.

Passphrases

Tiden for vanvittige og komplekse adgangskoder er forbi. Disse adgangskoder er svære at huske, vanskelige at taste, men med nutidens super hurtige computere er det nemt for IT-kriminelle at knække dem. Nøglen til sikre adgangskoder er at gøre dem lange, jo flere tegn jo bedre. Disse kaldes passphrases, en type adgangskode, der bruger en kort sætning eller tilfældige ord, hvilket gør adgangskoden stærkere. Her er to eksempler

Tid til stærk kaffe!
tabt-snegl-kravler-strand

Begge af disse er stærke med over tyve tegn, nemme at huske og enkle at skrive, men svære at knække. Du vil løbe ind på websteder eller situationer, der kræver, at du tilføjer symboler, tal eller store bogstaver til dit kodeord, hvilket er fint. Husk dog, at det er længden, der er vigtigst.

Password Managers

Du har brug for et unikt kodeord for hver konto. Hvis du genbruger den samme adgangskode til flere konti, udsætter du dig for en stor og unødvendig risiko. Alt en IT-kriminel skal gøre er at hacke et websted du bruger, stjæle alle adgangskoder, inklusive din, og derefter bruge dit kodeord til at logge ind på alle dine andre konti. Det sker langt oftere end du tror. Hvis du ikke tror på det kan du tjekke hjemmesiden www.haveibeenpwned.com for at se, hvilke af de websteder du bruger, der er blevet hacket og hvilke af dine adgangskoder der potentielt er kompromitteret. Så hvad skal du gøre? Brug en ”password manager”.

Dette er specielle computerprogrammer, der sikkert gemmer alle dine adgangskoder. Du behøver kun at huske en adgangskode, den ene til din password manager. Password manageren henter automatisk dine adgangskoder, når du har brug for dem, og logger dig ind på hjemmesider for dig. De har også andre funktioner som f.eks. at gemme dine svar på hemmelige spørgsmål,

advare dig, når du genbruger adgangskoder, en adgangskode generator, der sikrer at dine adgangskoder er sikre og mange andre funktioner. De fleste password manager synkroniserer også dine adgangskoder imellem dine enheder. Så uanset hvilket system du bruger, har du nem og sikker adgang til alle dine adgangskoder.

Endelig skal du skrive adgangskoden til din password manager ned og gemme den på et sikkert sted derhjemme. Nogle password manager har endda en løsning til dette. På den måde, hvis du glemmer adgangskoden til din password manager, har du en sikkerhedskopi. Eller hvis du bliver syg eller befinder dig i en nødsituation, kan din ægtefælle eller betroede familiemedlem hente oplysningerne på dine vegne.

To-trins verifikation

To-trins verifikation (ofte kaldet to-faktor verifikation, to-trinsbekræftelse eller flere-faktor verifikation) tilføjer et ekstra sikkerhedsniveau. Det kræver, at du har to ting, når du logger ind på dine konti, dit kodeord og en numerisk kode, der genereres af din smartphone eller som bliver sendt til din telefon. Denne proces sikrer, at selvom en IT-kriminel får din adgangskode, kan de stadig ikke komme ind på dine konti. To-trinsbekræftelse er nem at opsætte, og du skal normalt kun bruge den en gang, når du logger ind fra en ny computer eller enhed. Aktivér dette, når det er muligt, især for dine vigtigste konti, som f.eks. din bankkonto eller adgang til din e-mail. Hvis du bruger en password manager anbefaler vi kraftigt, at du beskytter den med en stærk passphrase OG to-trins verifikation.

Det kan lyde dumt, men med disse tre enkle trin når du langt i forhold til at beskytte dit job, omdømme og din økonomiske fremtid.

WelcomeSecurity samarbejder med netop din virksomhed om at identificere de IT sikkerhedsmæssige risici, som truer din virksomhed. Ved at analysere og teste jeres processer, teknologi og ikke mindst jeres medarbejder vil vi fastslå de mest effektive måder at minimere disse risici. Du kan finde os på https://www.welcomesecurity.net.

Gæsteredaktør

Justin Henderson *(@SecurityMapper) er medstifter af H & A Security Solutions, og er certificeret SANS Institut instruktør og forfatter til SANS "Cyber Defense" og "SIEM" kurser. Han elsker alle ting indenfor cyberforsvar og har været konsulent i femten år.*

Hvis du vil vide mere

Have I Been Pwned:	https://haveibeenpwned.com/
Two-factor Authentication Site:	https://twofactorauth.org/
NIST SP800-63B Digital Identity Guidelines:	https://pages.nist.gov/800-63-3/sp800-63b.html
Poster: You Are a Target:	https://www.sans.org/u/OGi