RESOURCE CENTER

Varje sekund räknas: 9 dagar för att fixa riskuppgifter är för långt

Två tredjedelar av IT-administratörerna säger att behörighetshantering är avgörande. Så varför saknar så många verktygen för att göra det? Ta reda på det i den senaste Bitwarden Business Insights-rapporten.

Get the full interactive view at https://bitwarden.com/sv-se/resources/bitwarden-business-insights-report/

bitwarden

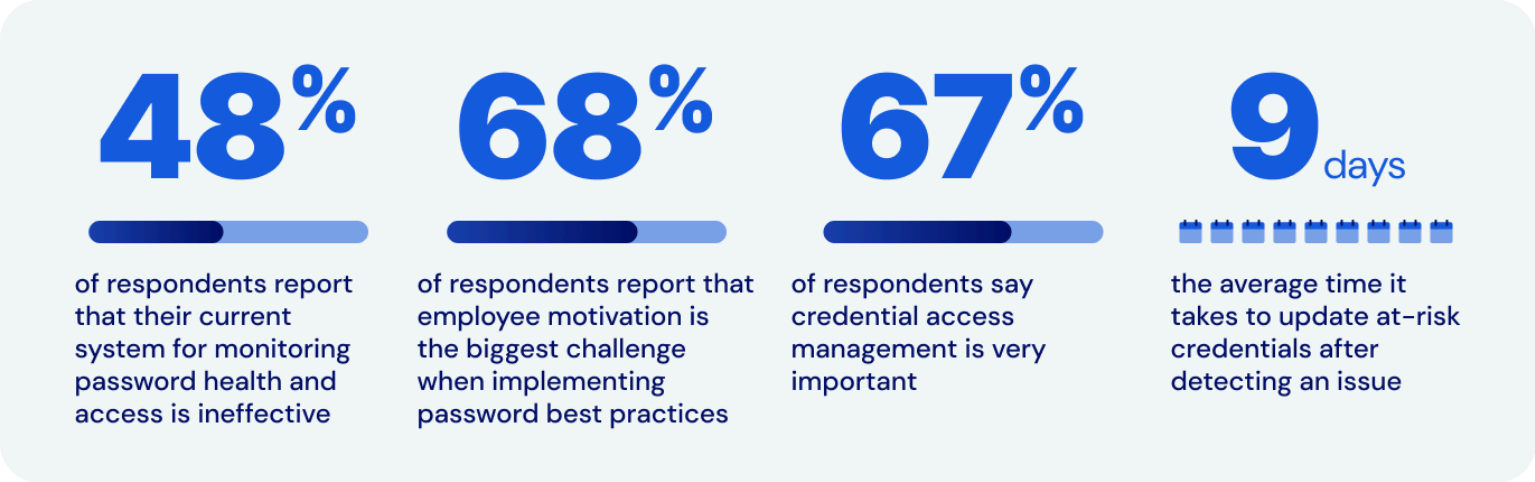
Sammanfattning

Svaga eller komprometterade lösenord är lätta att knäcka eller köpa på mörka webbmarknader. Dessa tunna inloggningsuppgifter är den digitala motsvarigheten till en ytterdörr med en nyckel kvar i låset: Det är trivialt för angripare att använda dem för att få olagligt inträde i en organisation.

Ändå är det en ständig utmaning att uppdatera dessa lösenord. IT-administratörer saknar ofta insyn i vilka lösenord som är svaga, återanvänds eller äventyrade. Även när de kan identifiera risklösenord kan det vara utmanande för dem att övertyga användare att uppdatera sina referenser eller ersätta dem med starkare. Dålig lösenordsövervakning kan också leda till okontrollerad åtkomst till känsliga, högprivilegierade system, vilket öppnar upp för ännu fler säkerhetsrisker för organisationen.

För att förstå detta landskap genomförde Bitwarden en undersökning av IT-chefer för att förstå deras smärtpunkter när det gäller synlighet och åtgärdande av lösenordshälsa. Dessa resultat sammanställdes i följande Bitwarden Business Insights 2025-rapport.

Nyckelfynd



En närmare titt: Behörighetsövervakning behövs, men ofta saknas eller saknas i den nuvarande verktygsuppsättningen

Två tredjedelar av de tillfrågade (67 %) säger att hantering av autentiseringsuppgifter är mycket viktigt för deras organisationer. Men nästan hälften (48 %) rapporterar att deras nuvarande system för att övervaka lösenordshälsa och åtkomst är ineffektivt.

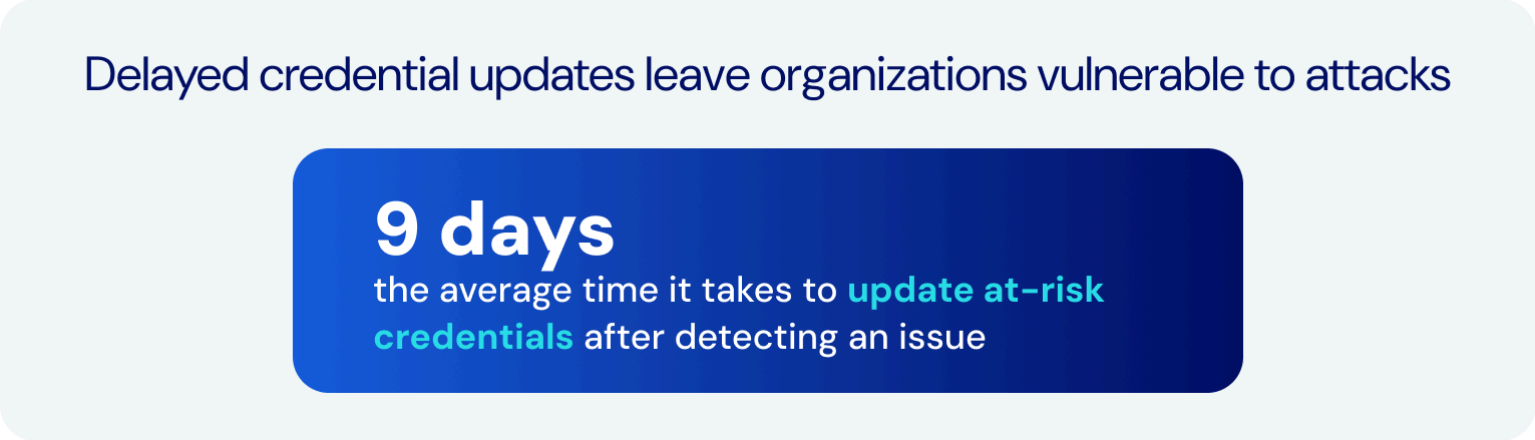
Denna brist på effektiv övervakning av lösenordshälsan och synlighet bidrar direkt till ouppfyllda säkerhetsmål och långsam upplösning.

Till exempel vill 53 % av IT-cheferna ta itu med legitimationsrelaterad säkerhet proaktivt, men bara 33 % säger att de gör det för närvarande. Ungefär 60 % av IT-cheferna säger att deras nuvarande strategi för att uppdatera autentiseringsuppgifter för risker i tid bara är något effektiv eller helt ineffektiv.

Vanligtvis (90 % av gångerna) ber respondenterna anställda att uppdatera sina egna referenser, och de gör detta oftast via e-post (42 %) eller en-till-en-konversationer (36 %).

Tyvärr rapporterar över hälften av IT-cheferna (51 %) att deras anställda inte alls eller bara tar cybersäkerhetsåtgärder på allvar.

Som ett resultat av detta tar anställda i genomsnitt 9 dagar på sig att uppdatera sina autentiseringsuppgifter för risker efter upptäckt, vilket lämnar dessa uppgifter som öppna sårbarheter för illvilliga aktörer att utnyttja. En organisation rapporterade att det tar ett helt år för anställda att uppdatera riskuppgifterna!



Motivation och prioritering: Nyckeln till förbättring

Den största utmaningen med att ändra detta utbredda problem med behörighetshantering och implementera bästa praxis för lösenord är att hitta ett sätt att motivera anställda att ändra sina vanor, vilket rapporterats av 68 % av de tillfrågade.

Medarbetarna själva kanske inte har de verktyg eller information de behöver. Bland IT-administratörer säger 44 % att anställdas förvirring om hur man gör lösenordsändringar är en utmaning, och 36 % klagar över svårigheter att spåra anställdas framsteg mot säkrare metoder.

Den främsta strategin för effektivare cybersäkerhet, som nämns av hälften av IT-cheferna (51 %), är att prioritera kritiska säkerhetsåtgärder tydligare. Dessutom skulle nästan hälften vilja se mer intuitiva arbetsflöden för icke-tekniska personer (46 %) och mer regelbunden säkerhetsutbildning (45 %). Fyrtio procent skulle vilja ha insyn i vem som inte har slutfört avgörande säkerhetsuppgifter.

Att kombinera effektiv prioritering, arbetsflöden och utbildning skulle hjälpa dessa chefer att bättre visa för anställda värdet av att ha säkra referenser – och skulle göra det möjligt för dem att fokusera på de referenser och privilegierade användare som är mest utsatta. Det skulle i sin tur hjälpa till att motivera anställda och minska tiden för att uppdatera svaga eller komprometterade lösenord. Att implementera dessa strategier kommer att hjälpa organisationer att bättre skydda sina affärsapplikationer, infrastruktur och konton från illvilliga aktörer.

Övervaka lösenordshälsan och hantera åtkomst över hela organisationen med Bitwarden

Bitwarden ger IT-team de verktyg de behöver för att säkert hantera sin organisations referenser med säkerhetslösningar för minst privilegierad åtkomst, lösenord, hemligheter och hantering av lösenord. Bitwarden litar på av tiotusentals företag och miljontals användare över hela världen, och gör det enkelt för anställda att anta starka lösenordspraxis och för administratörer att hantera organisationsvalv.

För organisationer som kämpar med att identifiera lösenordshälsa erbjuder Bitwarden valvhälsorapporter, som gör det möjligt för IT-administratörer att upptäcka autentiseringsuppgifter i riskzonen – inklusive exponerade, återanvända och svaga lösenord – kopplade till deras organisation. Detta är det första steget mot att stärka legitimationsrelaterad säkerhetsställning.

När riskuppgifter har identifierats och anställda underrättats, gör den inbyggda Bitwarden-lösenordsgeneratorn det möjligt för slutanvändare att snabbt ersätta en kränkande autentiseringsinformation med ett starkt, unikt lösenord och säkert spara det i företagets valv.

Ge dessa säkerhetsfunktioner en testkörning med en gratis 7-dagars Bitwarden affärstest!

Metodik

Bitwarden-undersökningen riktade sig till IT-administratörer och ägare på företag med mer än 1 miljoner USD i intäkter. Svar samlades in under slutet av 2024 och början av 2025 och fick totalt 108 svar.