



HR-tech-säkerhet

- skydda persondata i den digitala eran



Innehåll

Introduktion	3
Utmaningar inom HR-tech-säkerhet	4
Kapitel 1: Hotbild och risker inom HR-tech-säkerhet	5
Kapitel 2: Vikten av certifierad HR-tech-säkerhet	7
Kapitel 3: Checklista för att utvärdera HR-system	9
Kapitel 4: Säkerhet – en förutsättning för kvalitet och användarupplevelse	11
Kapitel 5: Skapa engagemang och utbilda internt i HR-säkerhet	13
• Varför är utbildning i HR-säkerhet viktigt?	13
• Strategier för att skapa engagemang	14
• HR som förebild i säkerhetskulturen	15
Kapitel 6: Sammanfattning och vägen framåt	16



Introduktion

Den snabba digitaliseringen av HR-processer har lett till en revolution inom hur företag hanterar och lagrar personaldata. HR-teknologi (HR-Tech) används idag för allt från rekrytering och onboarding till löneadministration och prestationshantering. En rapport från PwC visar att 74 % av organisationer planerar att öka sin investering i HR-Tech under de närmaste åren. Samtidigt visar en undersökning från ISACA att 30 % av HR-proffs saknar grundläggande kunskaper om cybersäkerhet, vilket skapar betydande risker.

Att skydda personaldata är kritiskt eftersom HR-system innehåller några av de mest känsliga uppgifterna i en organisation, inklusive personnummer, bankkonton, sjukjournaler och prestationsbedömningar. Bristande säkerhet kan leda till allvarliga konsekvenser, som dataintrång, identitetsstöld och juridiska sanktioner. Enligt IBM:s "Cost of a Data Breach Report" 2023 var den genomsnittliga kostnaden för ett dataintrång 4,45 miljoner dollar, och företag inom HR och rekrytering är särskilt sårbara på grund av den stora mängden personuppgifter de hanterar. Trots dessa risker saknar många organisationer en tydlig strategi för att hantera HR-tech-säkerhet.

Medan teknologiska framsteg som AI och molnbaserade system erbjuder förbättrad effektivitet och automatisering, medför de också nya säkerhetsutmaningar. Exempelvis kan AI-drivna rekryteringsplattformar samla in och analysera stora mängder data, men utan rätt säkerhetsåtgärder kan dessa system bli mål för cyberattacker.

För att säkerställa en trygg digital HR-miljö behöver företag investera i säkerhetsutbildning för HR-personal, införa robusta åtkomstkontroller och se till att alla system uppfyller gällande regulatoriska krav, såsom GDPR. Genom att kombinera teknologisk innovation med en stark säkerhetskultur kan organisationer skydda sin mest värdefulla tillgång – personaldata.



Utmaningar inom HR-tech-säkerhet

1. Dataintrång och cyberhot

- HR-system innehåller känslig information om anställda, inklusive personuppgifter, lön och sjukfrånvaro.
- Cyberattacker som phishing, ransomware och insiderhot kan leda till läckor av kritisk information.

2. Efterlevnad av GDPR och andra regelverk

- Företag måste säkerställa att persondata hanteras enligt gällande lagstiftning.
- Bristande efterlevnad kan leda till höga böter och rättsliga konsekvenser.

3. Tredjepartsleverantörer och molntjänster

- HR-plattformar från tredjepartsleverantörer kan utgöra en säkerhetsrisk om de inte uppfyller krav på dataskydd.
- Det är avgörande att genomföra riskbedömningar av externa system.





KAPITEL 1:

Hotbild och risker inom HR-tech-säkerhet

HR-teknologi har blivit en central del av moderna organisationer och effektiviserar allt från rekrytering och personalhantering till löneadministration. Med denna digitalisering följer dock en rad säkerhetsutmaningar. Eftersom HR-system hanterar stora mängder känslig information, inklusive personuppgifter, löner, sjukfrånvaro och anställningshistorik, har de blivit ett attraktivt mål för cyberkriminella. Dataintrång och informationsläckor kan inte bara leda till ekonomiska förluster utan även skada företagets rykte och förtroende.

En av de största säkerhetsriskerna inom HR-Tech är cyberattacker, där hackare använder metoder som phishing, ransomware och skadlig kod för att komma åt känslig information. En rapport från Verizon visar att nästan 34 % av alla dataintrång inom företag orsakas av interna hot eller mänskliga misstag, vilket gör att säkerhetsutbildning och strikt åtkomstkontroll blir avgörande för att minimera dessa risker. Utöver externa hot finns även risken för insiderhot, där anställda eller före detta anställda med tillgång till HR-system missbrukar sin position för att komma åt eller manipulera känsliga uppgifter. Bristfälliga åtkomstkontroller och svaga lösenordspolicys gör det ännu enklare för obehöriga att få tillgång till information de inte borde ha.

Vidare står HR-avdelningar inför en utmaning när det gäller efterlevnad av lagar och regelverk:

- GDPR och andra dataskyddsförordningar kräver att företag hanterar personuppgifter på ett säkert sätt.
- Många organisationer saknar tydliga rutiner för att säkerställa att de uppfyller dessa krav.
- Underlåtenhet att följa reglerna kan resultera i höga böter och allvarliga juridiska konsekvenser.
- Samarbete mellan HR, IT-säkerhetsteam och juridiska experter blir därför avgörande för att upprätthålla efterlevnad och skydda känslig information.





Många företag förlitar sig idag på molnbaserade HR-system, vilket ger flexibilitet och skalbarhet men också introducerar nya säkerhetsutmaningar. Tredjepartsleverantörer som hanterar HR-data kan utgöra en svag länk om deras säkerhetsåtgärder inte är tillräckligt robusta. Därför är det viktigt att genomföra noggranna riskbedömningar och säkerställa att leverantörerna följer de högsta säkerhetsstandarderna.

För att skydda HR-data krävs en kombination av tekniska lösningar och organisatoriska åtgärder. Tvåfaktorsautentisering, kryptering av data och regelbundna säkerhetsgranskningar är några av de tekniska åtgärder som kan minska riskerna. Samtidigt behöver HR-personal få kontinuerlig utbildning i cybersäkerhet för att undvika fallgropar som phishing-mejl och svaga lösenord. En kultur där säkerhet prioriteras på alla nivåer inom organisationen är avgörande för att skapa en trygg digital HR-miljö.

I takt med att AI och automatisering blir alltmer integrerade i HR-funktioner kommer säkerhetskraven att utvecklas ytterligare. Att proaktivt investera i robusta säkerhetslösningar och ständigt uppdatera skyddsstrategier är nödvändigt för att framtidssäkra HR-Tech och säkerställa att personaldata hanteras på ett tryggt och ansvarsfullt sätt.

KAPITEL 2:

Vikten av certifierad HR-tech-säkerhet

I en värld där cyberhoten ständigt utvecklas, är det avgörande att företag väljer HR-system som garanterar högsta möjliga säkerhetsstandard. Att arbeta med en plattform som är certifierad enligt ISO 27001:2022 innebär inte bara en tryggare hantering av känsliga personuppgifter utan även en förenklad efterlevnad av lagar och regelverk såsom GDPR. Certifieringen bekräftar att leverantören har implementerat strikta säkerhetsrutiner, vilket minimerar riskerna för dataintrång och informationsläckor.

ISO 27001:2022 är en globalt erkänd standard för informationssäkerhet som säkerställer att företag systematiskt identifierar, hanterar och minimerar säkerhetsrisker. För HR-system innebär detta att all persondata skyddas genom väl definierade processer och tekniska lösningar, från kryptering av information till strikt åtkomstkontroll och kontinuerliga säkerhetsrevisioner. Detta gör det betydligt enklare för organisationer att hålla sig inom ramarna för dataskyddslagstiftningen och undvika potentiella böter eller skador på sitt varumärke.

Ett av de största problemen inom HR-säkerhet är bristen på medvetenhet och förståelse för riskerna. En undersökning från ISACA visar att 30 % av HR-personal saknar grundläggande kunskaper i cybersäkerhet, vilket kan leda till oavsiktliga misstag och informationsläckor. Genom att använda en ISO 27001:2022-certifierad plattform kan företag minska risken för mänskliga fel genom inbyggda

säkerhetsåtgärder och användarvänliga funktioner som hjälper personalen att hantera känsliga data på ett tryggt sätt.

För företag som väljer en certifierad HR-lösning innebär det också att de kan lita på att säkerhetsarbetet kontinuerligt uppdateras och anpassas efter de senaste hotbilderna. Leverantörer med denna certifiering genomgår regelbundna externa granskningar och uppdateringar för att säkerställa att deras system uppfyller de senaste säkerhetskraven. Detta skapar en långsiktig trygghet och gör att organisationer kan fokusera på sin kärnverksamhet utan att ständigt behöva oroa sig för dataintrång eller säkerhetsluckor.





I en tid där cyberbrottsligheten ökar och dataskydd står högt på agendan, blir valet av en säker HR-plattform en strategisk investering. Genom att använda en ISO 27001:2022-certifierad lösning som exempelvis Heartpace HR, kan företag säkerställa att de arbetar med en plattform som inte bara är GDPR-säker utan också upprätthåller de högsta internationella standarderna för informationssäkerhet. Detta ger både arbetsgivare och anställda en ökad trygghet i hanteringen av personuppgifter, samtidigt som det förenklar organisationens säkerhetsarbete och efterlevnad av lagkrav.





KAPITEL 3:

Checklista för att utvärdera HR-system

När företag överväger att implementera ett nytt HR-system är det avgörande att säkerhetsaspekten tas på allvar redan från början. Här är en checklista som HR-avdelningar kan använda som vägledning vid utvärdering av olika system:

1. Efterlevnad och certifieringar

- ☐ Är systemet certifierat enligt internationella standarder för informationssäkerhet, såsom ISO 27001:2022?
- ☐ Uppfyller systemet GDPR och andra relevanta dataskyddslagar?

2. Säkerhetsfunktioner

- ☐ Erbjuder systemet tvåfaktorsautentisering för att stärka inloggningssäkerheten?
- ☐ Använder systemet kryptering för att skydda känsliga uppgifter både under överföring och lagring?
- ☐ Finns det loggning och spårbarhet av användaraktivitet?

3. Åtkomst och behörigheter

- ☐ Kan åtkomsträttigheter anpassas baserat på användarroller och specifika behov?
- ☐ Finns det en tydlig process för att hantera förändringar i anställningsstatus, såsom nyanställningar eller avslutade anställningar, för att säkerställa korrekt åtkomst?





4. Leverantörens säkerhetsrutiner

- ☐ Genomför leverantören regelbundna säkerhetsrevisioner?
- ☐ Har leverantören en tydlig incidenthanteringsplan vid dataintrång?

5. Användarvänlighet och utbildning

- ☐ Finns det utbildningsmaterial för HR-personal kring säker användning?
- ☐ Är systemet intuitivt och lätt att använda, vilket minskar risken för användarfel utan att kompromissa med säkerheten?

6. Integration och datahantering

- ☐ Hur hanteras data vid uppsägning av tjänsten? Finns det rutiner för säker radering eller återlämning av data?
- ☐ Kan systemet integreras säkert med befintliga IT-lösningar?

Genom att noggrant utvärdera dessa aspekter kan företag välja ett HR-system som inte bara är funktionellt och användarvänligt, utan också robust när det gäller säkerhet och dataskydd. Detta är avgörande för att skydda organisationens mest värdefulla tillgång – dess personaldata.

KAPITEL 4:

Säkerhet – en förutsättning för kvalitet och användarupplevelse

Ett HR-system kan ha en imponerande användarupplevelse och hög kvalitet, men utan rätt säkerhetsåtgärder är det i grunden osäkert. Att prioritera kvalitet och funktionalitet framför säkerhet är som att bygga ett lyxigt hus utan lås på dörrarna – det må vara vackert och bekvämt, men det är också en inbjudan till intrång.

Många företag frestas av lösningar som är enkla att implementera, smidiga att använda och estetiskt tilltalande. Men om säkerheten inte är inbyggd i systemets kärna blir det en riskfylld investering. Ett HR-system hanterar känsliga personuppgifter, och om dessa inte skyddas på rätt sätt kan det få allvarliga konsekvenser, både juridiskt och ekonomiskt. Dataintrång, identitetsstöld och informationsläckor kan orsaka skada som vida överstiger fördelarna med ett snyggt och användarvänligt gränssnitt.

Det finns många HR-system på marknaden som ser ut att uppfylla alla krav och erbjuder en tilltalande upplevelse för användaren. Men man får inte bli lurad av ett vackert yttre. Ett system kan ha en modern design, smidiga funktioner och god integration med andra plattformar – men utan en stark säkerhetsgrund är det inte en långsiktig lösning.

Därför är det viktigt att vara vaksam på varningstecken som tyder på att ett HR-system inte håller måttet när det gäller säkerhet:

1. Brist på transparens kring säkerhet – Om leverantören inte tydligt redogör för vilka säkerhetsåtgärder som finns på plats eller undviker att svara på frågor om efterlevnad av standarder som ISO 27001:2022 och GDPR, bör det vara en varningssignal.





2. Inga eller svaga autentiseringslösningar – Om systemet saknar funktioner som tvåfaktorsautentisering (2FA) eller Single Sign-On (SSO), är det ett tydligt tecken på att säkerheten inte är prioriterad.
3. Oregelbundna eller uteblivna säkerhetsuppdateringar – Ett system som inte genomgår regelbundna uppdateringar och säkerhetsrevisioner löper större risk att utsättas för cyberattacker och dataläckor.



Ett HR-system som har både hög säkerhet och utmärkt användarupplevelse är idealet, men säkerheten kan aldrig vara en eftertanke. Ett system som inte skyddar företagets och medarbetarnas information kan aldrig vara ett bra system – oavsett hur intuitivt och kraftfullt det är. Genom att välja en lösning där säkerhet är inbyggd från grunden kan företag säkerställa både trygghet och effektivitet i sin HR-hantering. ISO 27001:2022-certifierade system erbjuder just denna balans, där både säkerhet och kvalitet samverkar för att skapa en pålitlig och långsiktig lösning.



KAPITEL 5:

Skapa engagemang och utbilda internt i HR-säkerhet

För att säkerställa att företagets HR-system används på ett säkert sätt krävs inte bara robusta tekniska lösningar, utan också ett internt engagemang och medvetenhet kring IT-säkerhet. HR-avdelningen spelar en central roll i att driva denna förändring genom utbildning och tydliga riktlinjer. En undersökning från Gartner visar att endast 25 % av HR-avdelningar aktivt samarbetar med IT-säkerhetsteam för att skydda personaldata. Detta tyder på en kunskapslucka och ett behov av ökad medvetenhet inom HR om cybersäkerhetens betydelse.

Varför är utbildning i HR-säkerhet viktigt?

Trots att HR-system hanterar några av företagets mest känsliga data, saknar många organisationer strukturerade utbildningsinsatser inom IT-säkerhet för sina HR-medarbetare. Den mest avancerade säkerheten i system kan vara verkningslöst om medarbetarna inte vet hur de ska använda det på ett säkert sätt.



Strategier för att skapa engagemang

1. För att bygga en säkerhetsmedveten kultur i HR-avdelningen kan följande strategier användas:
Regelbundna säkerhetsutbildningar – Genom att hålla workshops och e-learningprogram om IT-säkerhet, GDPR och hur känsliga HR-data bör hanteras, kan företag höja medvetenheten och minska risken för misstag.
2. Simulerade phishing-attacker – Ett effektivt sätt att testa medarbetarnas vaksamhet är att genomföra simulerade nätfiskeattacker och sedan följa upp med utbildning baserat på resultaten.
3. Tydliga säkerhetsrutiner och policyer – HR bör skapa och kommunicera interna riktlinjer kring lösenordshantering, åtkomstkontroller och dataskydd för att säkerställa att alla vet vad som gäller.
4. Inkludera säkerhet i onboarding-processen – Nya HR-medarbetare bör redan från start få en grundläggande utbildning i IT-säkerhet och förstå vikten av att hantera HR-system på ett tryggt sätt.



HR som förebild i säkerhetskulturen

HR har en unik position i organisationen eftersom avdelningen ofta är ansvarig för både interna riktlinjer och medarbetarnas välmående. Genom att föregå med gott exempel och ständigt kommunicera vikten av säkerhet kan HR bidra till att skapa en företagskultur där IT-säkerhet är en självklar del av vardagen.

Att säkerhet är ett delat ansvar – där både IT-avdelningen, HR och alla anställda har en roll – är en insikt som behöver genomsyra hela organisationen. Genom att HR driver säkerhetsfrågor och säkerställer att medarbetarna är välinformerade kan risken för dataintrång och felhantering av känslig information minska avsevärt.



KAPITEL 6:

Sammanfattning och vägen framåt

I en digital värld där HR-system hanterar en stor mängd känsliga personuppgifter, kan säkerhet aldrig vara en sekundär prioritet. Vi har i denna whitepaper belyst hur HR-Tech-branschen måste kombinera starka säkerhetsåtgärder med en smidig användarupplevelse för att skapa hållbara, pålitliga och effektiva system.

Att välja rätt HR-system handlar om mer än bara funktionalitet och design. Det kräver en noggrann bedömning av säkerhetsstandarder, efterlevnad och leverantörens transparens kring cybersäkerhet. Ett tilltalande användargränssnitt och smarta funktioner får aldrig ske på bekostnad av skyddet för de anställdas data.

Framgångsrika organisationer bör ställa höga krav på sina HR-system och säkerställa att de är certifierade enligt internationella säkerhetsstandarder, såsom ISO 27001:2022. Genom att göra säkerhet till en grundläggande faktor i urvalsprocessen kan företag minimera riskerna och samtidigt dra nytta av innovativa och användarvänliga lösningar.

Slutligen är säkerhet inte en engångsinsats utan en kontinuerlig process. Tekniken utvecklas, hotbilder förändras och lagstiftningen uppdateras – därför måste HR-system kontinuerligt förbättras och anpassas. Genom att välja en leverantör som prioriterar säkerhet och håller sig i framkant av utvecklingen kan företag framtidssäkra sin HR-hantering och skapa en tryggare arbetsmiljö för sina anställda.





Vill du lära dig mer?

Är du intresserad av att lära dig mer om hur du kan stärka säkerheten i era HR-system men känner dig ännu inte redo att boka en demo? Tryck på 'Läs Mer' för att ta del av vår blogg där vi delar kunskap, tips, guider och insikter kring IT-säkerhet inom HR. Vi hjälper dig och din organisation att navigera i den digitala säkerhetsvärlden och skapa en tryggare hantering av känslig HR-data!

LÄS MER

Redo att säkra era HR-processer?

Vill du se hur ett säkert HR-system fungerar i praktiken? Boka en demo med oss på Heartpace och upplev hur vår ISO 27001:2022-certifierade plattform skyddar er mest känsliga data - utan att kompromissa med användarvänlighet. Under en demo visar vi hur ni kan säkerställa regelefterlevnad, minimera risker och bygga en säkerhetsmedveten HR-struktur.

BOKA EN DEMO

Heartpace HR är ett av Sveriges bäst betygsatta HR-system



