VDstödet
praktiska råd som fungerar

**Skydda Ditt Företag mot Dataintrång**

Data utgör ryggraden i ett företags verksamhet och skyddet av den informationen borde ha hög prioritet. Dataintrång innebär att någon utan tillstånd får tillgång till dina system och den information som finns där, helt eller delvis. I fel händer och med onda avsikter kan ett intrång därför få stora konsekvenser, ekonomiskt, juridiskt och organisatoriskt. Intrång kan ske av olika anledningar. Oaktsamhet med dokument, osäkra lösenord och bruten tystnadsplikt. Det kan bero på avsaknad av bra och uppdaterade program som kan hantera många hot och intrångsförsök. Det är viktigt att täcka in den teknik företaget använder, mobiler, plattor, pc och olika lagringsmedia för att identifiera obehörig åtkomst i tid. Nedan följer några viktiga åtgärder du kan vidta för att säkra ditt företags data och integritet.

**Identifiera** potentiella sårbarheter och hot mot företagets data genom regelbundna riskbedömningar. Utvärdera vilka typer av information som är mest känsliga och vilka system och processer som är mest utsatta. Dokumentera!

**Implementera** inloggning med två- eller flerstegsverifiering. Ett eller flera extra steg efter att lösenordet har angetts för att försvåra för obehöriga personer att få åtkomst till företagets system och data.

**Kryptera** all känslig information, både under lagring och överföring. På så sätt blir data oanvändbar för obehöriga även om den skulle komma i fel händer.

**Utbilda** alla anställda om säkerhetsprotokoll och bästa praxis för att undvika dataintrång. Nätfiske är idag en vanlig metod för angriparen att komma över lösenord eller bank- och kortuppgifter. Medvetenhetsträning kan minska risken för att anställda faller offer för social manipulationstekniker såsom nätfiske.

**Uppdatera** löpande alla program och system med de senaste programfixarna eller patchar som de kallas för att täppa till kända sårbarheter och minska risken för intrång.

**Begränsa** åtkomsten till företagets data och system endast till behöriga användare och endast på behovsbasis. Användarbehörigheter bör granskas och uppdateras regelbundet.

**Säkerhetskopiera** och upprätthåll säkerhetskopior av företagets data. På så sätt kan verksamheten snabbare återhämta sig från eventuella dataintrång eller katastrofer.

**Upprätta** en aktiv övervaknings- och reaktionsstrategi för att snabbt upptäcka och hantera eventuella hot eller intrångsförsök. Incidenthanteringsteam bör vara redo att agera snabbt vid eventuella säkerhetsincidenter.

**Säkerställ** att företaget följer alla relevanta lagar, regler och branschstandarder för dataskydd och integritet, t ex GDPR. Efterlevnad är avgörande för att undvika böter och rättsliga konsekvenser.

**Policy** som rör IT-säkerhet och handhavande. Den kan handla om allt från hur man lagrar filer på en USB-sticka, till hur man hanterar chattprogram och internet.
Genom en kombination av tekniska, utbildningsmässiga och processmässiga åtgärder kan du minimera risken att någon obehörig får tillgång till företagets system, nätverk och databaser.

jan.marcusson-stahl@vdstodet.se