

Dokumentssäkerhet: Hotade företag - hur dokumentssäkerhet kan skydda företagets konfidentiella uppgifter.

Adam Gillbe, Document Solutions Manager vid Canon Europa, tittar närmare på företagets konfidentialitet och då i synnerhet på dokumentssäkerheten inom europeiska företag. I artikeln hänvisar man till forskning utförd av ICM för Canon Europa, där man undersöker brott mot europeiska företagets konfidentialitet.

Hur säkert är ett genomsnittligt europeiskt företag? Vi börjar med de fysiska tillgångarna. Nästan alla företag har inbrottslarm, portkoder, brandlarm och försäkring. Men det är precis lika viktigt att skydda företagets immateriella tillgångar, däribland dokument som till exempel kontrakt, ekonomisk planering, strategiska dokument och personalinformation. Om fel personer får tillgång till det här kan det få stora konsekvenser för företaget och i värsta fall även leda till ekonomiska förluster.

Klientdokument med känslig information som läcks ut till pressen kan riskera att företagsryktet skadas och göra att affärsmöjligheter går förlorade för det företag som tros ha läckt informationen – för att inte tala om de åtal som klienten i fråga kan väcka. I sådana fall är det bättre att förekomma än förekommas. Om de anställda läser företagets konfidentiella information är det svårt att hindra dem från att diskutera informationen utanför kontorets väggar, och detta är något som nästan hälften av alla anställda i Europa har erkänt sig skyldiga till. I artikeln tittar vi närmare på hur företagen exponerar sig själva för den här typen av säkerhetskompromisser och hur man hanterar problemet.

Många företag skyddar sina konfidentiella dokument genom att säkra IT-systemen mot externa hot som virus, hackers och phishing. Men det skyddar inte mot interna brott mot dokumentssäkerheten. Interna säkerhetskompromisser börjar med bristande kunskaper på styrelse- och ledningsnivå när det gäller hoten mot dokumentssäkerheten. I genomsnitt 18 % av Europas företag ansåg att brott mot konfidentialiteten, eller "interna bedrägerier", var ett problem. 28 % ansåg att det var ett mindre problem. Men när vi då vet att fyra av tio anställda har sett känsliga affärsdokument och över en tredjedel gör det varje dag eller åtminstone varje månad, borde det här problemet ha en högre prioritet på styrelsens agenda. Om man ställer den här siffran i relation till det faktum att 82 % av cheferna vid europeiska företag tror att man kan "lita" på att de anställda inte avslöjar konfidentiell information och att detta är bästa sättet att förebygga problemet, inser vi hela vidden av problemet.

Dokumentsäkerhet får inte handla enbart om förtroende, eftersom ett förtroende inte ger några tydliga riktlinjer för vad som är ett brott mot företagets konfidentialitet. Om de anställda inte förstår vad som förväntas av dem kan de bryta mot konfidentialiteten utan att vara medvetna om det. Oavsett om brottet är avsiktligt eller ej, har det ändå hänt. 38 % av de anställda medgav att de hade sett känslig information eller visste att en kollega hade sett känslig information.

Att lägga in en paragraf om konfidentialitet i anställningskontraktet – som 64 % av Europas företag gör – räcker inte för att hindra anställda att öppet diskutera konfidentiell information, eftersom syftet med sådana paragrafer sällan eller aldrig förklaras för den anställde (och ännu mer sällan för tillfälligt anställda).

När det gäller skyddet av ett företags konfidentialitet måste man också tänka på de tillfälligt anställda, som finns med på många företags lönelistor, eftersom mindre än en fjärdedel av de europeiska företagen säger att de "alltid" gör säkerhetskontroller av tillfälligt anställda. Tillfälligt anställda anländer ofta till företaget med kort varsel, utan kontrakt och/eller introduktion. De kan eventuellt få tillgång till känsliga filer i företagets nätverk och skrivare, alternativt dokument som ligger öppet på kontoret. Antalet tillfälligt anställda som har tillgång till företagets skrivare varierar mellan 46 % i Storbritannien till endast 20 % i Österrike.

Ett första steg mot att skydda företagets immateriella tillgångar är att använda en godkänd konfidentialitetspolicy. Den måste då också förklaras för alla anställda, i syfte att minska möjligheterna och frestelserna att bryta mot företagets regler för informationssäkerhet.

Nästa steg, för att skydda företaget mot interna och externa hot mot dokumentsäkerheten, är att implementera IT- och skrivarsäkerhet. Nästan samtliga företag använder lösenord till enskilda anställdas datorer eller företagets nätverk. Vissa använder lösenordskontroller för åtkomst till delade nätverk, individuella skivenheter, filer och dokument. Men att bara skydda företagets datorer är en halvhjärtad åtgärd om tillgången till skrivarna inte skyddas också (vilket många företag inte gör). Skrivaren är ett viktigt verktyg som tyvärr ofta glöms bort när det gäller dokumentsäkerhet, men den borde ha hög prioritet när det gäller säkerheten och skyddas lika effektivt som en dator.

Det är i skrivaren som över en tredjedel av de anställda har sett företagets konfidentiella information. Bland informationen finns löne- och personalinformation, ekonomisk-, strategisk- och budgetplanering, som 88 % av de anställda säger sig ha sett. Dessutom trodde 21 % av de anställda att det var okej att läsa information som låg kvar i skrivaren/kopiatorn och 38 % av de anställda hade sett information i skrivare eller kopiatorer eller har kollegor som har gjort det.

Det finns flera sätt att skydda en företagsskrivare. Lösenord eller kort med magnetremsa är två kostnadseffektiva metoder för att kontrollera vem som skriver ut vad och när. Självklart måste företagen se till att ingen kan komma åt lösenorden. På marknaden finns även biometriteknik som har börjat anammas av vissa företag, speciellt inom finansvärlden där dokumentssäkerheten är av största vikt. Biometrisk kontroll, som till exempel fingeravtryck och näthinnescanning, är alternativa lösningar för att kontrollera skrivartillgången.

Utöver lösenordsskydd finns det även speciell programvara som kontrollerar dokumentutskriften på MFP-skrivarna. Denna installeras på en server och ger företaget möjlighet att se om ett dokument, i eller utanför kontoret, har visats, modifierats, flyttats eller distribuerats via skrivare, scanner eller fax, och av vem. Vissa lösningar innehåller även Triple Data Encryption Standard (DES) som skyddar dokumenten från obehörig åtkomst både inom och utanför en organisation. En annan fördel är att dokumenten får tydliga revisionsspår i företagets nätverk, genom de digitala signaturer som varje dokument tilldelas vid arkiveringen.

Via programvara kan företaget också fördela dokumentbehörighet, för att upprätthålla konfidentialitet, sekretess och ansvarsskyldighet. Detta innebär till exempel att olika dokumentprivilegier och -kryptering kan appliceras på olika dokumentåtkomstnivåer, som exempelvis PDF. Dokumentens ägare kan själva hantera dessa tillstånd och på så sätt skydda mot obehörig visning genom att kontrollera vem som kan öppna, redigera, skriva ut och kopiera respektive dokument. Åtkomsträttigheter för utskrift på en multifunktionsskrivare avgörs av vem som behöver åtkomst och på vilken nivå. En anställd, t.ex. en chef, kan ha tillstånd att läsa ett dokument och någon annan, t.ex. företagets styrelseordförande, kan ha tillstånd att skriva ut dokumentet.

Oavsett vilka metoder man använder för att skydda känsliga dokument bör dessa begränsade utskriftsmöjligheter följas upp av en genomtänkt dokumenthantering. För även om dokumenten öppnas och skrivs ut av rätt person, kan de ibland bli liggande i

skrivaren och kan då råka läsas av fel person. Här kan principen om det rena skrivbordet vara ett sätt att garantera att alla dokument arkiveras utom synhåll tills rätt person behöver dem, särskilt vid dagens slut.

Sådana här enkla steg kan, även om de inte är 100 % säkra, göra stor skillnad för ditt företags immateriella tillgångar, och det är hur som helst bättre än att basera företagets säkerhet på "förtroende". En tydlig och väl genomförd konfidentialitetspolicy innebär att man sätter en standard för godkänt beteende. Begränsad åtkomst för en MFP kan (precis som för företagets nätverk) förhindra onödigt snokande. Begränsad åtkomst till kontorets multifunktionsskrivare, och dokumentkontroll med hjälp av programvarulösningar, kan förhindra att känslig information – företagets immateriella tillgångar – hamnar i fel händer.