Informationssäkerhet

Texten nedan är allmänna råd framtagna av Sunet CERT kring hantering av viktig information inom organisationen, respektive organisation ansvarar för sin egen information.

Informationsklassning

Verksamhetens behov av skydd är ofta komplex och därför rekommenderas en jämn basnivå samt särskilda insatser för de system och information som har särskilda krav; så som studieinformationssystem, ekonomisystem och framförallt de forskningsprojekt som är av betydelse för andras vinning. En framgångsfaktor är att målgruppsanpassa de styrdokument som skapas så arbetet inte uppfattas som alltför resurskrävande eller irrelevant.

Msb har utvecklat ett metodstöd för systematiskt informationssäkerhetsarbete:

https://www.informationssakerhet.se/metodstod-for-lis/

Riskanalys och riskhantering

Oavsett insamlingsmetod eller bedömning av risker som skall åtgärdas är det viktigt att ta hänsyn till kvarvarande risk efter planerade åtgärder samt sätta ansvarig utförare och ägare kopplade till risken. Det är viktigt att kvalitetsproblem och bristande efterlevnad av rutiner inte ses som en procentuell sannolikhet utan att dessa hanteras av den ägare eller ansvarig där risken uppstår. Ett komplement till dessa bedömningar är att genomföra en GAP-analys utifrån verksamheten och omvärldens krav. ISO 27005 hanterar riskhantering för informationssäkerhet.

Utbildning och säkerhetsmedvetande

Att utbilda alla personer som befinner sig inom organisationen behöver ske kontinuerligt och vara särskilt riktat till nyanställningar och till de delar av organisationen där antingen riskvärdet är högt eller där kulturen har brister i acceptansen för de gemensamma baskraven för hur man hanterar andras data. Exempel på detta är: delade användarkonton, olåsta utrymmen till känsligt material eller riskfyllt beteende på internet.

Spionage

Många länder bedriver underrättelseverksamhet (spionage). Oavsett vad drivkraften är så kan universitetet och lärosäten vara direkt mål utifrån den information som skapas eller behandlas. Det kan också vara en språngbräda utifrån de nätverk som finns. Såväl fysiska datornätverk som mänskliga samverkansnätverk. Allt för många säkerhetsansvariga vet om fall där utländska personer ertappas stå och kopiera texter från pärmar eller ladda ned stora mängder data. Att låsa fysiska utrymmen som inte behöver vara öppna ligger utanför vad Sunet CERT rådgiver inom men är en viktig faktor för att hålla obehöriga borta då inga andra personer befinner sig i lokalerna. Denna kultur skiljer sig mycket mellan olika lärosätes riskacceptans.

Mer info:

http://www.sakerhetspolisen.se/kontraspionage/sa-fungerar-kontraspionage.html

https://www.svd.se/svenska-universitet-utsatta-nar-spionage-okar

Identitetshantering

En viktig aspekt kring nyttjande av it-resurser vid lärosäten är att fastställa identiteten för användare. Då kan större friheter ges mellan lärosätens resurser och forskning kan bedrivas mer effektivt. Internet är idag mer hotfullt än hur det såg ut i samband med att lärosätena kopplade samman sig med olika tjänster. Därför behövs en starkare koppling mellan digital identitet och faktisk person.

Mer information:

https://www.sunet.se/swamid/policy/

Åtkomstsbegränsning av känslig utrustning

Institutionsplacerad utrustning inom naturvetenskapliga områden är ofta svår att upprätthålla säkerheten på då sårbarheter i protokoll eller gränssnitt lämnas trasiga antingen för att supportavtal inte fullföljs eller att leverantören inte utvecklar skydd mot dessa nyupptäckta hot. Ett sätt att skydda dessa utrustningar är att placera dem på egna nätverk, antingen via VPN eller bakom accesslistor. Samma problem gäller även för skrivarlösningar där problemet kanske enbart uppfattas som obehöriga utskrifter men dagens multifunktionsskrivare är servrar med hårddiskar som kan nyttjas för vidare attacker inom och utom lärosätet.

Övervakning, detektion och åtgärd

Att ha relevant loggdata är inte enbart en compliance fråga. Det är en förutsättning för att kunna hitta och identifiera missbruk och angrepp mot den tekniska miljön. Att kunna agera automatiskt på angrepp och händelser är en framgångsfaktor.

Relevanta skydd för en öppen miljö

Universitetsvärlden är fantastisk på det sätt samverkan kan ske. Stödjande arkitekturprinciper och delade resurser skapas långt innan många delar av internet och företag anpassat sig. Kring administrativ IT och de stödsystem som finns förflyttas ibland information ut via molntjänster. Det är viktigt att informationsklassning sker så rätt legala förutsättningar finns för personuppgiftsbiträdesavtal och ägandeskap av informationen. Det är därför viktigt att de inloggnings och behörighetsmekanismer som finns att kravställning sker gemensamt så kontroll över den kan bestå.

Andra handfasta tips så som att ha bra systemuppdateringar, säkerhetskopior samt att begränsa rättigheter till det som krävs ligger utanför dessa råd och återfinns inom ISO 27000 standarden.