LINEE GUIDA SULLA SICUREZZA INFORMATICA

Premessa

L'Istituto di Ricerca sugli Ecosistemi Terrestri (IRET) è un'istituto del CNR composto da 6 strutture:

• Sede di Porano, ubicata in Via G. Marconi N. 2, 05010 Porano (TR).
• Sezione di Montelibretti presso Area di Ricerca Roma 1 – Strada Provinciale 35d, 9 - 00010, Montelibretti (RM).
• Sezione di Napoli in Via P. Castellino n. 111, 80131 Napoli (NA).
• Sezione di Pisa in Via Moruzzi n. 1, 56124 Pisa (PI).
• Sezione di Firenze in Via Madonna del Piano n.10, 50019 Sesto Fiorentino (FI).
• Sezione di Sassari in Traversa La Crucca n. 3, 07100 Sassari (SS).

Dato il particolare rilievo che i sistemi informatici assumono nel funzionamento dell'Istituto, in particolare per lo svolgimento dell'attività di ricerca, organizzativa e gestionale, in relazione con le quali viene effettuato anche il trattamento di dati personali, è obiettivo di assoluta priorità salvaguardare la sicurezza del proprio sistema informatico e tutelare la riservatezza, l'integrità e la disponibilità delle informazioni, prodotte, raccolte o comunque trattate, da ogni minaccia intenzionale od accidentale, interna od esterna all'Istituto.
In tale contesto si intende per

• ***tutela della riservatezza***: la riduzione del rischio che una qualsiasi entità possa accedere alle informazioni senza esserne autorizzata;
• ***tutela dell'integrità***: la riduzione del rischio che i dati o le informazioni siano modificati o distrutti;
• ***tutela della disponibilità***: la riduzione del rischio che l'accesso ai dati ed alle informazioni possa essere impedito ai soggetti autorizzati.

Il riferimento alla riduzione del rischio, e non alla eliminazione dello stesso, è dovuto alla consapevolezza della impossibilità di raggiungere in ambito informatico una condizione di sicurezza assoluta.

I rischi e le minacce al Sistema Informatico

Il Sistema Informatico dell'Istituto è composto dalle apparecchiature (quali computer, stampanti e apparati di rete), dal software e dai dati utilizzati per le varie attività istituzionali.
La predisposizione di adeguate misure di sicurezza richiede consapevolezza dei rischi e delle minacce cui può essere sottoposto un sistema e a tal fine IRET ha effettuato un'analisi dei potenziali eventi lesivi.
Si intende per minaccia un qualsiasi evento non desiderato, sia volontario che accidentale, idoneo ad arrecare danno, direttamente o indirettamente, al Sistema Informatico.
Le minacce più comuni si individuano come segue:

• ***danneggiamenti***: eventi di origine naturale o derivante da comportamenti umani, in grado di arrecare danno;
• ***furti***: appropriazione da parte di terzi di hardware, software, dati e informazioni appartenenti all'Ente;

• ***frodi*** o malversazioni: azioni poste in essere attraverso inganni, raggiri o contraffazioni e dirette ad ottenere profitti illeciti, personali o di terzi;
• ***manipolazioni di dati o programmi***: azioni dirette a modificare, in modo non autorizzato, i dati ed i programmi;
• ***perdita di privacy e riservatezza***: eventi accidentali o deliberati, idonei a determinare l'accesso ad informazioni riservate da parte di soggetti non autorizzati;
• ***divulgazioni di dati e/o programmi***: azioni ritenute intermedie tra gli atti di frode e il furto poste in essere non attraverso la sottrazione del bene, ma mediante copia non autorizzata dello stesso e successiva divulgazione;
• ***uso illecito di risorse hardware e software***: utilizzazione non autorizzata o abusiva delle risorse informatiche dell'Istituto;
• ***malfunzionamenti del sistema***: eventi strettamente connessi al sistema in grado di comprometterne l'affidabilità e la continuità dei servizi;
• ***inagibilità dei locali***: condizioni di impraticabilità dei locali in cui sono posti gli archivi offline o dove sono svolte le attività;
• ***minacce provenienti da Internet e dalle reti***: aggressioni al sistema informatico determinate o agevolate dal collegamento degli elaboratori a reti informatiche quali ad esempio:

- azioni dirette ad utilizzare i difetti e le debolezze dei protocolli di trasmissione dei dati; ad es.: denial of service, insieme di tecniche per provocare malfunzionamenti o blocchi del sistema informatico;
- azioni dirette ad utilizzare difetti esistenti nei meccanismi di autenticazione e autorizzazione;
- azioni dirette ad inserirsi in una rete locale senza la necessaria autorizzazione, in particolare nel caso di reti wireless, per le quali è necessario prevedere configurazioni particolarmente curate a causa delle difficoltà di circoscrizione geografica;
- azioni dirette a sfruttare difetti ed errori del software (bug) o ad usare funzionalità non note agli utilizzatori (backdoor);
- furto di password;
- virus e worm informatici: programmi eseguibili capaci di riprodursi copiando loro stessi all'insaputa e senza l'autorizzazione dell'utente: attualmente costituiscono una tra le più diffuse minacce al sistema informatico;
- phishing: il tentativo di ottenere l'accesso a informazioni personali e riservate mediante l'utilizzo di messaggi di posta elettronica, opportunamente creati per apparire autentici.

Obiettivi di sicurezza

In relazione alle minacce indicate ed ai conseguenti potenziali rischi, IRET ritiene necessario adottare idonee misure dirette a garantire la sicurezza del sistema informatico nel suo complesso; misure che attengono secondo la tripartizione convenzionalmente accolta:
• la sicurezza fisica,
• la sicurezza logica,
• la sicurezza organizzativa.

Sicurezza fisica
Con riferimento a tale aspetto, connesso alla protezione dei locali, delle risorse umane e delle componenti hardware e software che costituiscono il sistema informatico aziendale, IRET prevede:
• un servizio di vigilanza presso ciascuna delle strutture ed apposite convenzioni con le Università per tutelare la sicurezza dei luoghi nelle Strutture situate presso le sedi universitarie, al fine di ridurre il rischio di furti e danneggiamenti connessi a condotte umane volontarie;
• sistemi anti-intrusione con procedure d'ingresso controllato nei locali che ospitano i server ed elaboratori, mediante i quali vengono trattati dati personali, al fine di ridurre il rischio di furto, danneggiamento, perdita della riservatezza e divulgazione specialmente per i dati e le informazioni per le quali la legge richiede una particolare riservatezza (art.9 del regolamento Europeo 679/2016 (GDPR) – recepita dall'ordinamento nazionale attraverso il d.lgs 101/2018 Adeguamento Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE);
• la predisposizione di dispositivi antincendio e di continuità elettrica in modo tale da ridurre il rischio di danneggiamenti e malfunzionamenti di quelle parti del sistema ritenute critiche al fine di garantire l'espletamento delle attività dell'istituto.

Sicurezza logica
Rappresenta una forma di tutela direttamente connessa alla protezione dei dati e delle informazioni e si esplica in misure tecnologiche dirette a garantire riservatezza, integrità, autenticità, non-ripudio e disponibilità.

Riservatezza (*Confidentiality*).
Dati e informazioni memorizzate in un sistema o scambiate tra due entità devono essere protette da letture non autorizzate, ovvero devono risultare accessibili solo agli utenti e ai processi che ne hanno diritto, in base alle policy definite nel sistema. La riservatezza, nota anche come segretezza o confidenzialità, si ottiene principalmente mediante tecniche crittografiche.

Integrità (*Integrity*).
Dati e informazioni memorizzate in un sistema o scambiate tra due entità devono essere protette da modifiche non autorizzate (alterazione, cancellazione o aggiunta). L'integrità può essere garantita da meccanismi di checksum, da tecniche crittografiche come la firma digitale, oltre che da meccanismi per il controllo dell'accesso ai dati.

Autenticità (*Authenticity*).
Chi riceve un messaggio deve poterne identificare con certezza la provenienza, ossia verificare l'identità dell'origine. Parallelamente l'utente o un'altra entità, al fine di ottenere l'accesso a un servizio deve preliminarmente dimostrare la propria identità presso il sistema che ospita tale servizio (autenticazione)

Non ripudiabilità (*Non repudiation*).
Chi genera un messaggio non deve poter negare successivamente di averlo generato, né deve poterne negare il contenuto. Allo stesso modo, chi riceve un messaggio non deve poter negare di averlo ricevuto, né deve poterne negare il contenuto. La non ripudiabilità è ottenuta attraverso

tecniche crittografiche.

Disponibilità (*Availability*).
Le risorse, i servizi e i dati di un sistema devono essere sempre accessibili agli utenti legittimi. I sistemi devono risultare funzionanti con il livello di prestazioni prestabilito. Le minacce intenzionali più comuni a questa proprietà sono per esempio gli attacchi denial of service, I cali di tensione, guasti all'hardware, disastri naturali.

A tal fine IRET ha adottato le Misure Minime di Sicurezza ICT per le pubbliche amministrazioni indicate da AGID con la circolare n. 2/2017 del 18 aprile 2017 pubblicata nella Gazzetta Ufficiale Serie Generale n.103 del 05-05-2017.

Sicurezza organizzativa
E' relativa all'individuazione delle procedure dirette alla implementazione, gestione e controllo delle misure di sicurezza adottate e si concretizza:

1. nell'individuazione di ruoli, funzioni e responsabilità coinvolte nella realizzazione e gestione del sistema di sicurezza, con riferimento alla tutela sia dei dati di carattere scientifico sia dei dati personali, conformemente a quanto disposto dal Codice in materia di tutela dei dati personali;
2. nell'individuazione delle procedure da seguire per conservare in sicurezza il sistema informatico, regolamentando la condotta degli utenti.

Con riferimento al punto 1 l'articolazione organizzativa in ciascuna struttura prevede:
• Il Direttore o un Responsabile di Sezione, cui compete il funzionamento scientifico, organizzativo ed amministrativo della Struttura; il direttore è individuato, con riferimento al trattamento dei dati personali, Responsabile Interno CNR del Trattamento (Provvedimento n.27 del 2019, ai sensi dell'articolo 2, quaterdecies, comma 1, del decreto legislativo 30 giugno 2003, n.196).
• Il Gruppo Referenti Informatici, con privilegi di Amministratore di sistema, cui competono la gestione delle risorse hardware e software, i collegamenti in rete all'interno ed all'esterno della Struttura, nonché la cura, installazione e sviluppo delle stesse e l'assistenza agli utenti per l'accesso alle risorse ed alla rete; ha inoltre competenza in materia di sicurezza su ogni risorsa hardware e software comunque afferente alla propria Struttura;
• Gli Utenti, soggetti che hanno accesso alle risorse di elaborazione e ai servizi di rete, in relazione alle funzioni ed attività che sono chiamati a svolgere in ambito di Istituto; gli utenti autorizzati al trattamento dei dati personali sono individuati come incaricati del trattamento ai sensi dell' art. 4, n. 10 e art. 29 del GDPR.

Per quanto attiene il punto 2, l'individuazione delle procedure viene formalizzata attraverso le Policy di Istituto in materia di sicurezza informatica e specifici regolamenti di condotta, periodicamente aggiornati in relazione all'evoluzione tecnologica del settore.
Compiti di coordinamento nell'individuazione delle politiche di sicurezza e nell'adozione delle conseguenti misure sono affidati al Gruppo Referenti Informatici.
L'IRET attribuisce particolare rilievo alla costante sensibilizzazione degli utenti ad un uso corretto

delle risorse informatiche, attraverso attività di formazione ed aggiornamento, dirette a creare, al di là di competenze specialistiche proprie dei soggetti tenuti alla gestione del sistema, un patrimonio comune di conoscenze informatiche relativamente alle nozioni basilari di protezione, manutenzione ed uso degli elaboratori.

Verifica dell'adeguatezza delle misure di sicurezza

L'IRET verifica periodicamente l'adeguatezza ed efficacia delle misure di sicurezza adottate provvedendo ad adeguare le stesse alla particolare evoluzione tecnologica del settore, al fine di mantenere elevato il livello di protezione e ridurre, quindi, il livello di rischio.
L'attività di verifica viene attuata mediante procedure di monitoraggio e di audit ed in particolare:
• attraverso un sistema di monitoraggio effettuato dal gruppo dei referenti informatici che eseguono un controllo costante dell'effettivo funzionamento del sistema informatico e delle misure di sicurezza, adottando tutte le misure necessarie ad incrementarne il livello di efficacia;
• attraverso la previsione di un'attività di audit, quale controllo saltuario svolto da soggetti diversi dai referenti informatici, al fine di ottenere un giudizio imparziale circa la qualità delle misure di sicurezza approntate ed in grado di evidenziarne eventuali debolezze od errori.

CALFAPIETRA
CARLO
27.01.2020
11:57:17 UTC