Tecnologie satellitari e sicurezza: lo spazio come nuova frontiera cyber

Mercoledì 24 maggio 2023

Seminario online 9:30 – 12:30

“La Cyber Security nel contesto dell’ITU”

Mauro Di Crescenzo – Radio Regulation Board Member

LO SCENARIO DI RIFERIMENTO

- Negli anni 80-90 si stimava che le reti satellitari fossero sicure dagli attacchi informatici in virtù delle loro caratteristiche intrinseche quali la tipologia di accesso e l'architettura del sistema.
- Oggi questo concetto è superato e le organizzazioni internazionali che operano nel settore satellitare stanno collaborando per migliorare il livello della sicurezza informatica non solo al proprio interno ma anche in tutto il settore di riferimento, contribuendo a rendere le comunicazioni più resistenti agli attacchi e ad accelerare l'integrazione dei sistemi e dei servizi spaziali con quelli terrestri.
- La maggior parte di queste organizzazioni potrebbe essere vulnerabili agli attacchi ai propri dati o reti, spesso attraverso internet, ma anche attraverso segnali radio o altre modalità.
- Le minacce alla sicurezza si manifestano abitualmente attraverso attacchi mirati a punti generici della rete, mentre in alcuni casi sono specificamente dirette contro un nodo della rete considerato più vulnerabile.
- Le telecomunicazioni possono essere interrotte con segnali bloccanti, o nel caso di sistema di navigazione satellitare attraverso l'introduzione di dati errati.
- I sistemi di comunicazione satellitare si stanno diffondendo sempre di più e le applicazioni spaziali sono fondamentali per l'ampia e crescente gamma di servizi che offrono sia nel settore civile che militare, quali ad esempio la sicurezza in mare, la radionavigazione, le osservazioni meteorologiche, il monitoraggio delle variazioni climatiche, lo stato degli oceani e tante altre applicazioni.

PROTEGGERE I CONTENUTI

- Per loro natura le comunicazioni satellitari comprendono aree geografiche molto ampie ed è molto probabile che la sicurezza delle informazioni coinvolga numerose nazioni.
- Per proteggere l'integrità e la riservatezza delle informazioni che viaggiano sulle reti satellitari, in un contesto così articolato, occorre studiare e proporre dei meccanismi di protezione condivisi globalmente.
- Questo obiettivo può essere raggiunto interessando organizzazioni internazionali, in cui partecipano un numero significativo di paesi e che quindi possiedono un elevato grado di influenza.
- L'ITU è una di queste organizzazioni con la specifica responsabilità di proteggere gli interessi degli stati membri, che operano nel settore delle ICTs e quindi anche nella tecnologia spaziale, assicurando un adeguato livello di protezione e garantendo la continua disponibilità delle informazioni condivise.

THE INTERNATIONAL TELECOMMUNICATION UNION (ITU)

The International Telecommunication Union (ITU) è l'Agenzia delle Nazioni Unite (193 paesi membri) specializzata per le tecnologie delle informazioni e comunicazioni (**Information and Communication Technologies – ICTs**).

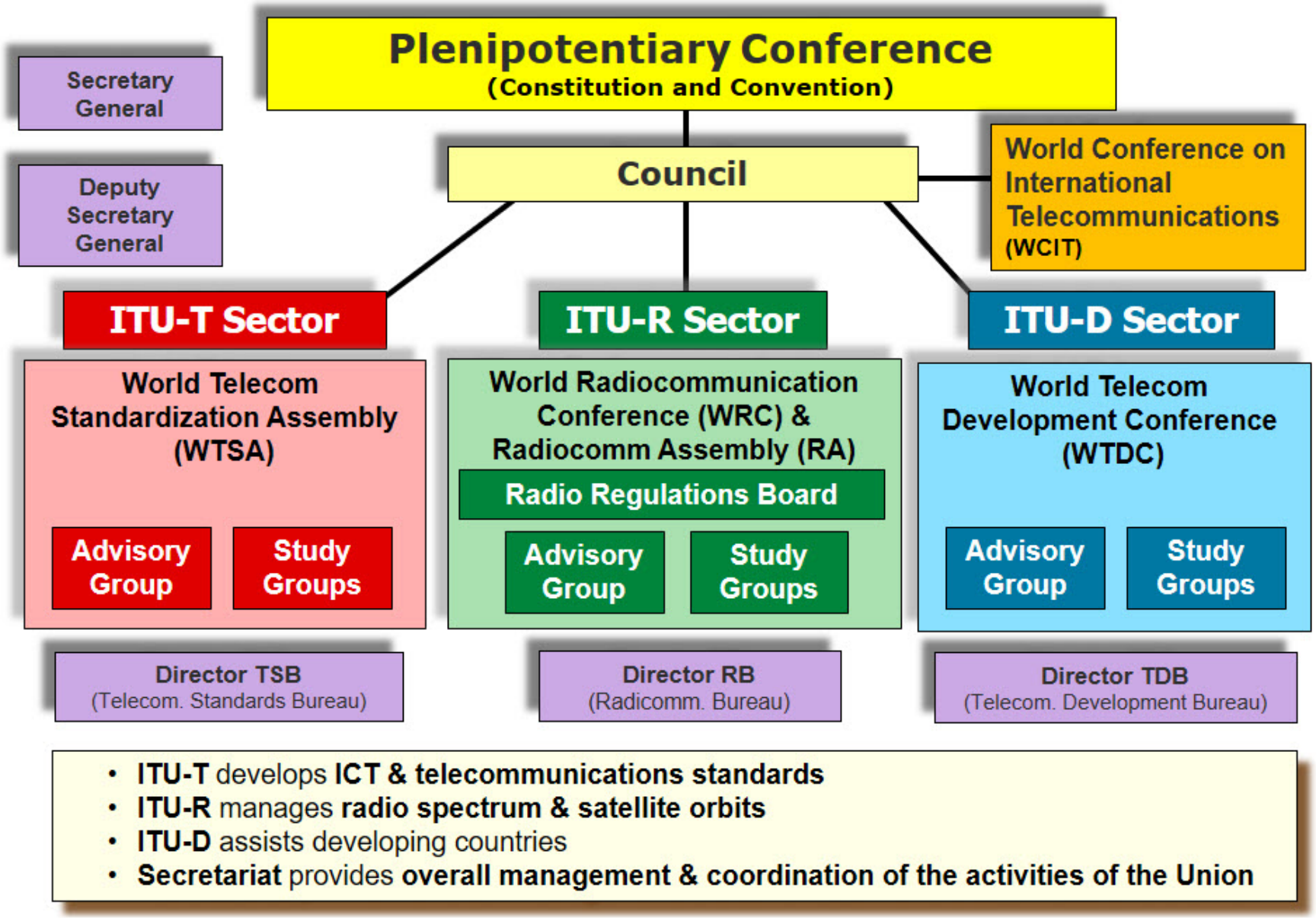
Fondata nel 1865 per facilitare la connettività internazionale nelle reti di comunicazione, assegna lo spettro radio globale e le orbite satellitari, sviluppa gli standard tecnici che garantiscono l'interconnessione delle reti e delle tecnologie e si adopera per migliorare l'accesso ICTs alle comunità di tutto il mondo ed in particolare a quelle in via di sviluppo.

L'ITU svolge le proprie attività in linea con il suo mandato e le raccomandazioni emerse negli atti finali del Forum annuale della World Summit on the Information Society (WSIS).

L'ITU ha tre principali aree di attività organizzate in "Settori" che operano attraverso conferenze e gruppi di studio:

RADIOCOMMUNICATIONS, STANDARDIZATION AND DEVELOPMENT

L'ORGANIGRAMMA DELL'ITU



ISED's Involvement in the International Telecommunication Union: Evaluation report (June 2020) Innovation, Science and Economic Development Canada

I SETTORI DELL'ITU

RADIOCOMMUNICATIONS - Il Radiocommunication Sector (ITU-R) dell'ITU coordina i servizi di radiocomunicazione e la gestione internazionale dello spettro delle radiofrequenze e delle orbite satellitari. A causa dell'enorme richiesta, queste risorse sono limitate e partecipare alle conferenze ITU-R e alle attività dei gruppi di studio - in cui vengono svolte attività tecniche e normative, sta diventando una priorità sempre più alta sia per i governi che per gli operatori del settore.

STANDARDIZATION - Telecommunication Standardization Sector (ITU-T) produce gli standard ITU (chiamati raccomandazioni) che sono fondamentali per il funzionamento delle reti ICT. Senza gli standard ITU non si potrebbe fare una telefonata o navigare in Internet. Centinaia di standard ITU, impiegati per l'accesso a Internet, per i protocolli di trasporto, per la compressione voce e video, per le reti domestiche e molte altre applicazioni delle ITC, consentono ai sistemi di funzionare, a livello locale e globale. Come ad esempio, lo standard ITU-T H.264 che è diventato uno degli standard più popolari per la compressione video. Nell'arco di un anno l'ITU elabora e produce circa 150 standard che interessano le funzionalità di rete ed i servizi di prossima generazione.

DEVELOPMENT - Telecommunication Development Sector (ITU-D) ha la missione di agevolare l'introduzione delle tecnologie ICT nei paesi in via di sviluppo facilitando gli operatori del settore ad entrare o espandere la propria presenza nei mercati emergenti. L'ITU sostiene una serie di importanti iniziative che comprendono il mandato internazionalmente concesso all' ITU di "colmare il divario digitale", attraverso eventi a carattere promozionale. L'ITU pubblica regolarmente le statistiche ICT. In un mondo sempre più interconnesso, ampliare l'accesso alle ITC a livello globale è nell'interesse di tutti.

IL SETTORE ITU-T

Le attività del settore della Standardizzazione consistono nello sviluppare Recommendations (standards) Internazionali per i vari campi di applicazione delle Telecomunicazioni.

Il lavoro viene svolto da gruppi di studio tecnici (SGs) in cui partecipano i membri dell'ITU-T, provenienti dalle varie Amministrazioni (ITU-T membership)

- SG2 - Operational aspects
- SG3 - Economic & policy issues
- SG5 - Environment, EMF & circular economy
- SG9 - Broadband cable & TV
- SG11 - Protocols, testing & combating counterfeiting
- SG12 - Performance, QoS & QoE
- SG13 - Future networks
- SG15 - Transport, access & home
- SG16 - Multimedia & digital technologies
- **SG17 – Security**
- SG20 - IoT, smart cities & communities

Il Gruppo di Studio 17 (SG17) coordina le attività in ambito della sicurezza svolte da tutti i gruppi di studio ITU-T, operando in collaborazione con altre organizzazioni di sviluppo degli standard e vari consorzi industriali del settore ICT.

IL GRUPPO DI STUDIO 17 (SG17)

Il ruolo del gruppo di studio 17 consiste nel fornire soluzioni tecniche per comprendere e garantire la sicurezza in ambito ITC.

Gli studi si concentrano in particolare sulla sicurezza delle reti che operano in contesti innovativi quali International Mobile Telecommunications (IMT/5G), Internet of Things (IoT), città intelligenti, Distributed Ledger Technology (DLT), analisi dei big data, Intelligent Transportation Systems (ITS), intelligenza artificiale (AI) e tecnologie relative alla quantistica.

Le sue aree di studio includono anche la gestione delle informazioni di identificazione personale (PII), come gli aspetti tecnici e operativi della protezione dei dati per garantire la riservatezza, l'integrità e la disponibilità delle PII.

Il gruppo di studio 17 è quindi responsabile dell'elaborazione delle raccomandazioni principali sulla sicurezza dell'ITC, quali l'analisi dell'architettura di riferimento; lo studio dei principi della cyber-security (minacce, vulnerabilità e rischi), la gestione/risposta agli incidenti e il recupero dei dati danneggiati.

Inoltre il gruppo di studio 17 è responsabile della gestione delle PII, per la protezione dei dati e per l'individuazione dei mezzi tecnici in grado di contrastare i messaggi di posta elettronica non richiesti (spam).

AREE TEMATICHE - APPLICAZIONI E SERVIZI

Le attività dello SG17 possono essere viste logicamente attraverso una connessione tra aree tematiche e fornitura di applicazioni/servizi. A titolo di esempio le tabelle ipotizzano delle possibili connessioni fra aree tematiche e le applicazioni/servizi

Aree Tematiche:

- sicurezza informatica in contesti innovativi;
- gestione degli incidenti e recupero dei dati danneggiati;
- architetture di riferimento per la sicurezza;
- contrasto allo spam;
- gestione dell'identità, protezione delle informazioni di identificazione personale;
- aspetti operativi della protezione dei dati;
- framework di fiducia dell'identità aperta;
- sicurezza quantistica;
- protezione online dei minori;
- …….

Applicazioni e servizi:

- Internet of Things (IoT),
- smart grid;
- smartphone,
- networking definito dal software;
- servizi web;
- analisi dei big data;
- social network;
- cloud computing;
- sistemi finanziari mobili;
- IPTV, tecnologia di registro distribuito;
- sistema di trasporto intelligente;
- Tele biometria;
- Lotta alla contraffazione e al furto di dispositivi mobili;
- IMT/5G;
- sanità elettronica;
- identificazione a radiofrequenza;
- …….

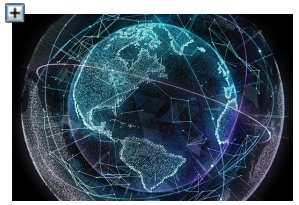
RACCOMANDAZIONI ITU-T SOTTO LA RESPONSABILITA' DELLO STG17

- **SG17 Recommendations**
  - **E series**: Overall network operation, telephone service, service operation and human factors
  - **F series**: Non-telephone Telecommunication services
  - **X series**: Data networks, open system communications **and security**
  - **Z series**: Languages and general software aspects for telecommunication systems

I gruppi di studio dell'ITU-T, a causa della complessità degli argomenti trattati, hanno una struttura articolata e di non facile lettura. La tematica satellitare non è confinata in uno specifico documento o trattata direttamente ma può essere dedotta da più trattazioni distribuite nelle varie serie ed in differenti aree all'interno di esse.

X SERIES: DATA NETWORKS, OPEN SYSTEM COMMUNICATION AND SECURITY

- **X series: Data networks, open system communications and security**
  - X.200-X.299: Open Systems Interconnection
  - X.400-X.499: Message Handling Systems
  - X.500-X.599: Directory
  - X.600-X.699: OSI networking and system aspects
  - X.800-X.849: Security
  - X.850-X.899: OSI applications
  - X.900-X.999: Open distributed processing
  - X.1000-X.1099: Information and network security
  - X.1100-X.1199: Secure applications and services (1)
  - X.1200-X.1299: Cyberspace security
  - X.1300-X.1499: Secure applications and services (2)
  - X.1500-X.1599: Cybersecurity information exchange
  - X.1600-X.1699: Cloud computing security
  - X.1700-X.1729: Quantum communication
  - X.1750-X.1799: Data security
  - X.1800-X.1819: IMT-2020 Security
  - X Supplements: Supplements to ITU-T X-series Recommendations



X.1200-X.1299: CYBERSPACE SECURITY

- **X.1200-X.1229**: Cyberspace security
- X.1205: Overview of cybersecurity
- X.1206: A vendor-neutral framework for automatic notification of security related information and dissemination of updates
- X.1207: Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software
- X.1208: A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies
- X.1209: Capabilities and their context scenarios for cybersecurity information sharing and exchange
- X.1210: Overview of source-based security troubleshooting mechanisms for Internet protocol-based networks
- X.1211: Techniques for preventing web-based attacks
- X.1212: Design considerations for improved end-user perception of trustworthiness indicators
- X.1213: Security capability requirements for countering smartphone-based botnets
- X.1214: Security assessment techniques in telecommunication/information and communication technology networks
- X.1215: Use cases for structured threat information expression
- X.1216: Requirements for collection and preservation of cybersecurity incident evidence
- X.1217: Guidelines for applying threat intelligence in telecommunication network operation
- X.1218: Requirements and guidelines for dynamic malware analysis in a sandbox environment
- **X.1230-X.1249**: Countering spam
- **X.1250-X.1279**: Identity management

LA RACCOMANDAZIONE ITU-T X.805

La Raccomandazione ITU-T X.805 definisce il concetto di un'architettura di rete in grado di fornire comunicazioni end-to-end sicure.

L'architettura può essere applicata a vari tipi di reti in cui la sicurezza end-to-end è un elemento di criticità ed è indipendentemente dalla tecnologia utilizzata.

La Raccomandazione definisce alcuni elementi generali e si pone l'obiettivo di essere considerata come base per lo sviluppo di raccomandazioni più dettagliate applicabile ad uno contesto simile. Il concetto di architettura di rete sicura è applicabile a reti wireless, comunicazioni vocali su cavo, trasmissioni di dati, linee ottiche e reti convergenti ovvero integrate.

Il concetto di rete sicura analizza le problematiche di sicurezza per la gestione, controllo e utilizzo dell'infrastruttura di rete, dei servizi e delle applicazioni. Il concetto di base consiste nel dividere logicamente l'architettura di rete in un insieme complesso di componenti separati. Questa separazione consente un approccio sistematico che può essere utilizzato per la pianificazione di specifiche soluzioni valutando l'efficacia delle misure esistenti.

L'ARCHITETTURA DI RIFERIMENTO

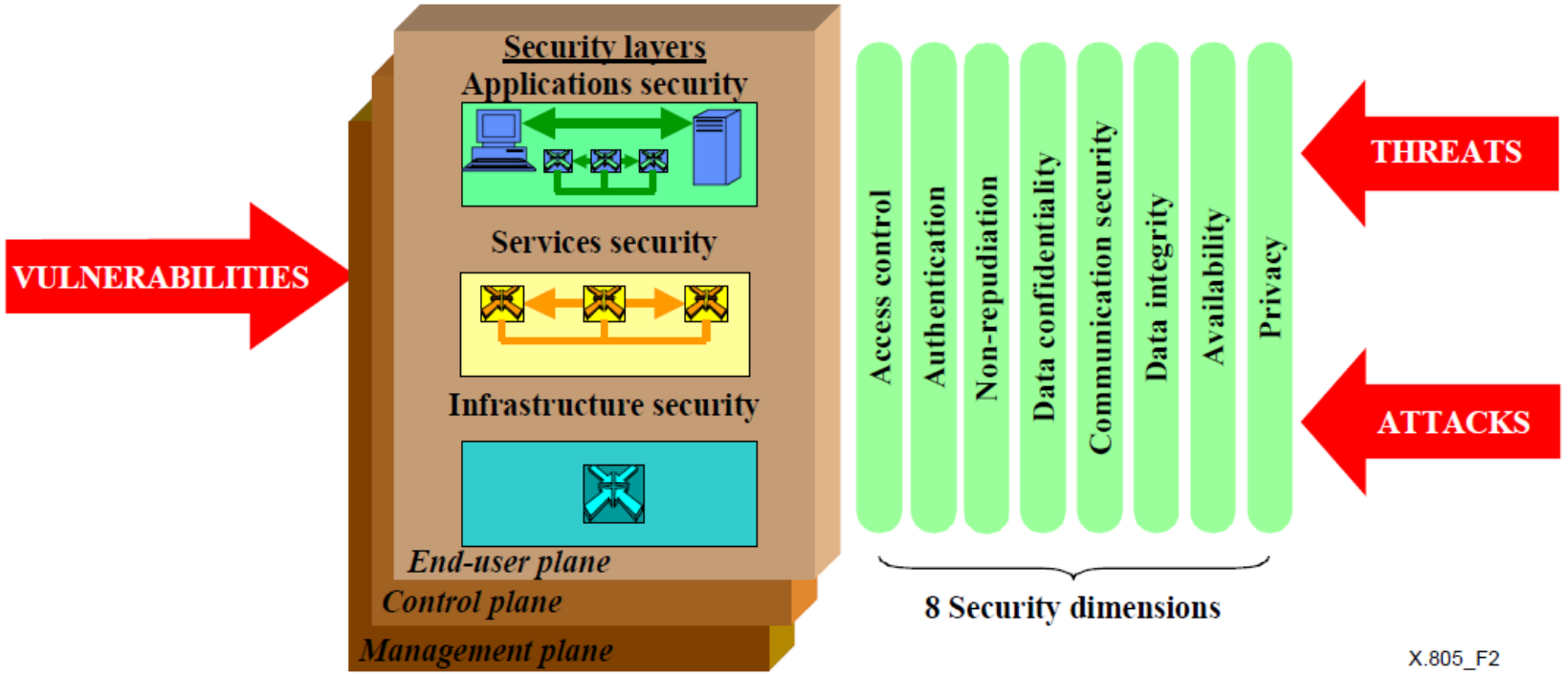


Figure 2/X.805 – Security planes reflect the different types of network activities

LA RACCOMANDAZIONE ITU-T X.1205

La raccomandazione ITU-T X.1205 fornisce una definizione per la Cyber Security presentando una tassonomia delle minacce alla sicurezza presenti in una tipica organizzazione pubblica o privata.

La raccomandazione descrive quindi le minacce e le vulnerabilità per la sicurezza informatica, inclusi gli strumenti più comuni utilizzati dagli hacker per violare l'obiettivo individuato.

La trattazione si articola analizzando, ai differenti livelli di rete, le varie tecnologie disponibili per porre rimedio alle potenziali minacce, tra cui: router, firewall, protezione antivirus, sistemi di rilevamento delle intrusioni, sistemi di protezione dalle intrusioni, metodologie di accesso al sistema, controllo e monitoraggio della rete.

La raccomandazione introduce dei principi di protezione della rete, come la difesa sistematica e la gestione degli accessi tramite applicazioni specifiche di protezione. Oggetto della raccomandazione è inoltre l'analisi delle strategie e delle tecniche di gestione del rischio di cui parte integrante consiste nel valorizzare il ruolo della formazione evidenziando l'importanza di applicare le disposizioni individuate per la protezione della rete. La raccomandazione fornisce e analizza esempi sulle tecnologie proposte.

LA DEFINIZIONE DI CYBER SECURITY

Rec. ITU-T X.1205 (04/2008)

……..

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

……

3.2.3 cryptographic algorithm: A cryptographic algorithm is the means by which data are altered and disguised in encryption.

3.2.4 cyber environment: This includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks.

3.2.5 cybersecurity: Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality.

……..

INTERPRETAZIONE DELLA DEFINIZIONE DI CYBER SECURITY

La Cyberseurity è la raccolta di strumenti, politiche, concetti, tutele, linee guida, metodologie di gestione del rischio, azioni, formazione, migliori pratiche, garanzie e tecnologie che possono essere utilizzate per proteggere l'ambiente informatico a tutela del patrimonio dell'organizzazione e del singolo utente.

Il patrimonio dell'organizzazione e del singolo utente include i dispositivi informatici connessi, il personale, l'infrastruttura, le applicazioni, i servizi, i sistemi di telecomunicazione e la totalità delle informazioni trasmesse e/o archiviate nell'ambiente informatico.

La Cybersecurity si impegna a garantire il raggiungimento e il mantenimento delle sicurezza delle proprietà informatiche dell'organizzazione e dell'utente contro i rischi ad essa associati. Gli obiettivi generali di sicurezza comprendono: • Disponibilità; • Integrità; • Riservatezza.

L’IMPORTANZA DELLE RACCOMANDAZIONI

- Definiscono uno scenario di riferimento che è l’oggetto della raccomandazione;
- Stabiliscono termini e definizioni;
- Identificano delle procedure operative;
- Propongono le modalità di applicazione delle procedure identificate;
- Pianificano ulteriori approfondimenti;
- Forniscono esempi per facilitare la comprensione degli argomenti trattati

The World Telecommunication Standardization Assembly (WTSA)

La World Telecommunication Standardization Assembly (WTSA) si tiene ogni quattro anni per definire gli studi che l'ITU-T dovrà realizzare nel periodo di riferimento. L'ultima Assemblea (WTSA-20) si è tenuta a Ginevra a Marzo 2022 preceduta dal Global Standards Symposium (Febbraio 2022).

Il Global Standards Symposium (GSS) è organizzato dall'ITU e consiste in un forum di alte professionalità, anche non appartenenti alle Amministrazioni che aderiscono all'ITU, per discutere le modalità con cui tutti i soggetti interessati potrebbero collaborare per sviluppare gli standard internazionali, le linee guida ed il contesto di riferimento che dovrà sostenere la trasformazione digitale per gli obiettivi di sviluppo sostenibile (Sustainable Development Goals - SDGs).

In conformità con la Risoluzione 122 (Rev. Guadalajara, 2010) della Conferenza plenipotenziaria e la Risoluzione 1272 (MOD) del Consiglio dell'ITU, le conclusioni del GSS-20 dettagliate in questo rapporto sono trasmesse per esame al WTSA-20 .

I risultati della WTSA-20 sono contenuti nei proceedings e comprendono le Resoluzioni, le Opinioni e le Raccomandazioni discusse durante la conferenza.

La versione finale di tutte le Risoluzioni ed Opinioni si può trovare sul sito dell'ITU Resolutions and Opinions (itu.int).

Le Raccomandazioni sono riportate all'indirizzo ITU-T Recommendations

World Summit on the Information Society Forum (WSIS) 2023

Il Forum WSIS è telematico, sostenuto e preparato grazie all'impegno profuso dagli enti governativi, dal settore privato, dal mondo accademico, dalla comunità tecnica e dalle organizzazioni intergovernative che ne garantisce la titolarità ed i continui miglioramenti. L'agenda e il programma del forum sono costruiti sulla base delle proposte ufficiali ricevute durante un processo di consultazione aperta a tutti. In una delle sessioni è stato discusso il seguente argomento a testimonianza del crescente interesse verso le tematiche satellitari:

" Working together to sustain our future: what space has to offer and how we protect it

This session brings highly respected experts together to talk about their involvement in the context of space, and how they view the merits of space activities to our lives on Earth. A key feature of this session relates to 'international cooperation' and sharing the benefits of space for humankind. It is an interactive session - wherein various questions are posed to the experts - our experts being from the EU; US and other parts of the globe and working in areas such as GNSS (Galileo and Egnos for example) and other cooperative activities.

This session only too clearly evidences the benefits of space to us on Earth, in so much as it aids to connect all parts of the globe and, therefore, is an essential foundation for advancing ICT."

Session 311— Working together to sustain our future: what space has to offer and how we… | WSIS Forum 2023 (itu.int)

LA RISOLUZIONE 50 (interpretazione-1)

Le attività dell'ITU-T sulla Cyber security sono descritte nella risoluzione 50 così come aggiornata nell'ultima World Telecommunication Standardization Assembly (WTSA)

" RESOLUTION 50 (Rev. Geneva, 2022) Cybersecurity "

La risoluzione si articola in diverse parti:

Nei "resolves " (decisioni) si evidenziano i punti:

1. continuare ad attribuire alla Cybersecurity un'elevata priorità all'interno dell'ITU-T, conformemente alle sue competenze ed esperienze, promuovendo una visione condivisa tra i governi e le altre parti interessate per incentivare l'utilizzo delle procedure di sicurezza nelle ICTs a livello nazionale, regionale e internazionale;

4. che l'ITU-T dovrebbe diffondere la percezione sull'efficacia del rispetto delle norme sulla sicurezza a livello globale nelle ICTs attraverso lo sviluppo di raccomandazioni e relazioni tecniche a sostegno delle procedure di sicurezza informatica, delle specifiche tecniche e dei riferimenti normativi;

8. che dovrebbero essere promossi processi globali, coerenti e interoperabili per la condivisione delle informazioni relative alla risposta agli incidenti;

9. che i gruppi di studio ITU-T continuino a mantenere i contatti con le organizzazioni normative e altri organismi attivi in questo campo ed incoraggino l'impegno di esperti nelle attività dell'ITU sul tema della sicurezza delle ICTs;

12. che il gruppo di studio 17 deve sviluppare, su basi cooperative un'analisi sulla gestione degli incidenti relativi alla sicurezza.

LA RISOLUZIONE 50 (interpretazione-2)

Nella parte “*instructs Study Group 17*“ che rappresenta un indirizzamento al gruppo di studio 17 si evidenziano i punti:

5. definire un insieme comune di procedure di sicurezza, per ogni fase del ciclo dei vita di sistemi informativi, delle reti e delle applicazioni, in modo che si possa raggiungere, fin dal momento della progettazione, un elevato grado di attenzione sugli aspetti legati alla sicurezza;
6. progettare architetture di riferimento, per la componente relativa alla sicurezza, da considerare come piattaforme base per la progettazione di sistemi, reti ed applicazioni personalizzati e più complessi ed in modo che possano contribuire a migliorare la qualità delle specifiche raccomandazioni.

LA RISOLUZIONE 50 (interpretazione-3)

Nella parte " instructs the Director of the Telecommunication Standardization Bureau "

1. continuare a mantenere, sulla base della base di quanto stabilito nei programmi di sviluppo degli standard di sicurezza in ambito ICTs, dal contributo dell'UIT-D e con l'assistenza di altre organizzazioni, un inventario delle iniziative e delle attività nazionali, regionali e internazionali per promuovere, per quanto possibile, l'armonizzazione mondiale delle strategie e delle iniziative in questo settore di vitale importanza, senza perdere di vista lo sviluppo di pratiche comuni per la Cybersecurity;

5. attuare e garantire il proseguimento delle attività del WSIS volte a rafforzare la diffusione e l'utilizzo delle politiche di sicurezza nell'ambito delle ICTs, in collaborazione con gli altri settori dell'ITU e in cooperazione con gli stati membri, in modo da condividere informazioni e pratiche in ambito nazionale, regionale ed internazionale, per favorirne un utilizzo globale e non discriminatorio.

LA RISOLUZIONE 50 (interpretazione-4)

Nella parte "invites Member States, Sector Members, Associates and Academia, as appropriate"

2. cooperare e partecipare attivamente all'attuazione della presente risoluzione e delle azioni associate;
3. partecipare alle attività dei gruppi di studio ITU-T per sviluppare norme e orientamenti in materia di Cybersecurity al fine di incentivare l'utilizzo delle procedure di sicurezza nelle ICTs;
4. utilizzare le raccomandazioni ITU-T in modo appropriato;
5. continuare a contribuire ai lavori del gruppo di studio 17 sulle attività inerenti alla gestione del rischio informatico.

LA RISOLUZIONE 50

resolves

1. **to continue to give this work high priority within ITU-T, in accordance with its competencies and expertise, including promoting common understanding among governments and other stakeholders of building confidence and security in the use of ICTs at the national, regional and international level**;
2. that all ITU-T study groups continue to evaluate existing and evolving new Recommendations, with respect to their robustness of design and potential for exploitation by malicious parties, and take into account new services and emerging applications to be supported by the global telecommunication/ICT infrastructure (including, but not limited to, for example, cloud computing and IoT, which are based on telecommunication/ICT networks), according to their mandates in Resolution 2 (Rev. Geneva, 2022) of this assembly;
3. that ITU-T continue to raise awareness, within its mandate and competencies, of the need to harden and defend information and telecommunication systems from cyberthreats and malicious cyberactivity, and continue to promote cooperation among appropriate international and regional organizations in order to enhance exchange of technical information in the field of information and telecommunication network security;

LA RISOLUZIONE 50

4. **that ITU-T should raise global awareness regarding security in ICTs through the development of Recommendations and technical reports which support cybersecurity procedures, technical policies and standards frameworks**;
5. that ITU-T should work with ITU-D, particularly in the context of ITU-D Question 3/2 (Securing information and communication networks: Best practices for developing a culture of cybersecurity);
6. that relevant ITU-T study groups should keep pace with the development of the new and emerging technologies, according to their mandates, in order to develop Recommendations, supplements and technical reports that help to overcome challenges related to security;
7. that ITU-T continue work on the development and improvement of terms and definitions related to building confidence and security in the use of telecommunications/ICTs, including the term cybersecurity;
8. **that global, consistent and interoperable processes for sharing information related to incident response should be promoted**;
9. **that ITU-T study groups continue to liaise with standards organizations and other bodies active in this field and encourage the engagement of experts in ITU's activities in the area of building confidence and security in the use of ICTs**;
10. that security aspects should be considered throughout the ITU-T standards-development process;
11. that secure, trusted and resilient telecommunication/ICT networks and services should be developed and maintained to enhance confidence in the use of ICT;
12. **that Study Group 17 needs to develop cooperative security analysis and incident management frameworks;**
13. that the resilience of ICT networks and systems should be considered as a priority in network and infrastructure development,

LA RISOLUZIONE 50

instructs Study Group 17

1. to promote studies on cybersecurity, including security for new services and emerging applications to be supported by the global telecommunication/ICT infrastructure;
2. to support the Director of TSB to maintain the ICT Security Standards Roadmap, which should include work items to progress standardization work related to security, and share this with relevant groups of the ITU Radiocommunication Sector (ITU-R) and ITU-D as the mission of the lead group for security;
3. to promote joint coordination activities on security among all relevant study groups and focus groups in ITU and other standards-development organizations;
4. to collaborate closely with all other ITU-T study groups, establish an action plan for assessing existing, evolving and new ITU-T Recommendations to counter security vulnerabilities, and continue to provide regular reports on security of telecommunications/ICT to the Telecommunication Standardization Advisory Group;
5. **to define a general/common set of security capabilities for each phase of information system/network/application lifecycles, so that consequently security by design (security capabilities and features available by design) could be achieved for systems/networks/applications from day one;**
6. **to design one or more security architecture reference frameworks with security functional components which could be considered as the basis of security architecture design for various systems/networks/applications in order to improve the quality of Recommendations on security,**

LA RISOLUZIONE 50

instructs the Director of the Telecommunication Standardization Bureau

1. **to continue to maintain, in building upon the information base associated with the ICT Security Standards Roadmap and ITU-D efforts on cybersecurity, and with the assistance of other relevant organizations, an inventory of national, regional and international initiatives and activities to promote, to the maximum extent possible, the worldwide harmonization of strategies and approaches in this critically important area, including the development of common approaches in the field of cybersecurity;**
2. to contribute to annual reports to the ITU Council on building confidence and security in the use of ICTs, as specified in Resolution 130 (Rev. Dubai, 2018);
3. to report to the Council on the progress of activities on the ICT Security Standards Roadmap;
4. to continue to recognize the role played by other organizations with experience and expertise in the area of security standards, and coordinate with those organizations as appropriate;
5. **to continue the implementation and follow-up of relevant WSIS activities on building confidence and security in the use of ICTs, in collaboration with the other ITU Sectors and in cooperation with relevant stakeholders, as a way to share information and best practices on national, regional and international non-discriminatory cybersecurity-related initiatives globally**;

LA RISOLUZIONE 50

6. to cooperate with the Secretary-General's GCA and other global or regional cybersecurity projects, as appropriate, in promoting capacity building and developing relationships and partnerships with various regional and international cybersecurity-related organizations and initiatives, as appropriate, and to invite all Member States, particularly developing countries, to take part in these activities and to coordinate and cooperate with these different activities;
7. to support the Director of the Telecommunication Development Bureau (BDT) in assisting Member States in the establishment of an appropriate framework among developing countries allowing rapid response to major incidents, and to propose an action plan to increase their protection, taking into account mechanisms and partnerships, as appropriate;
8. to support relevant ITU-T study group activities related to strengthening and building confidence and security in the use of ICTs;
9. to disseminate information to all stakeholders related to cybersecurity through the organization of training programmes, forums, workshops, seminars, etc., for policy-makers, regulators, operators and other stakeholders, especially from developing countries, to raise awareness and identify needs in collaboration with the Director of BDT,

LA RISOLUZIONE 50

invites Member States, Sector Members, Associates and Academia, as appropriate

1. to collaborate closely in strengthening regional and international cooperation, taking into account Resolution 130 (Rev. Dubai, 2018), with a view to enhancing confidence and security in the use of ICTs, in order to mitigate risks and threats;
2. **to cooperate and participate actively in the implementation of this resolution and the associated actions;**
3. **to participate in relevant ITU-T study group activities to develop cybersecurity standards and guidelines in order to build confidence and security in the use of ICTs;**
4. **to utilize relevant ITU-T Recommendations and supplements;**
5. **to continue to contribute to Study Group 17 work on cyberrisk-management approaches.**