BITRON GROUP

THE INFORMATION SECURITY MANAGEMENT SYSTEM
(i.e. THE HACKERS HOLY GRAIL)

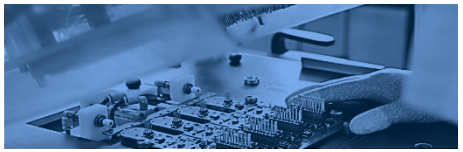
Febbraio, 2018





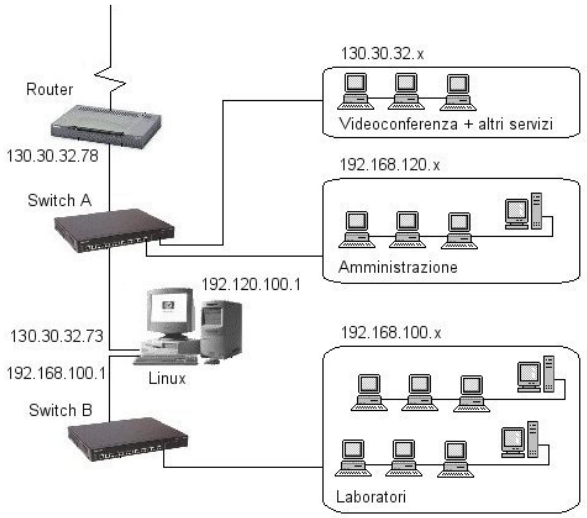





La Sicurezza delle Informazioni: l'evoluzione della comunicazione

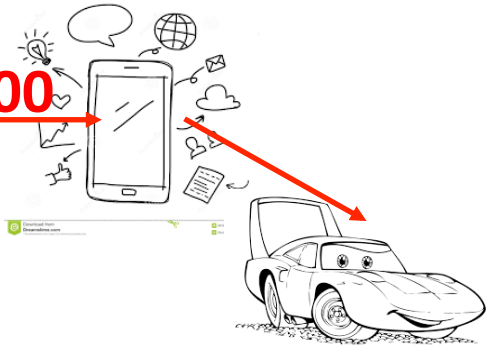
1980 RETI MILITARI E UNIVERSITARIE (ARPANET)

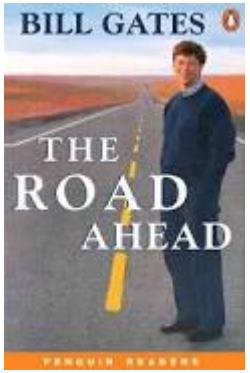


1990 INTERNET

WWW

2000





NEL 2025 TUTTE LE NUOVE AUTOVETTURE SARANNO EQUIPAGGIATE CON SIM E CONNESSE IN RETE.

IL PERICOLO CHE INFORMAZIONI RISERVATE CADANO NELLE MANI SBAGLIATE E CHE MALINTENZIONATI POSSANO PRENDERE IL CONTROLLO DELLA VETTURA E' SEMPRE PIU REALE

I PIU' IMPORTANTI OEM AUTOMOTIVE STANNO RICHIEDENDO AI LORO FORNITORI DI GARANTIRE LA SICUREZZA DELLE INFORMAZIONI SCAMBIATE CON LORO IN OTTEMPERANZA ALLE LEGGI ED ALLE OBBLIGAZIONI CONTRATTUALI.

FCA FIAT CHRYSLER AUTOMOBILES

Mercedes-Benz

Il Sistema di Gestione della Sicurezza delle Informazioni

- **IL SISTEMA DELLE INFORMAZIONI È GENERALMENTE DEFINITO COME L'INSIEME DEI DATI E DELLE RISORSE HARDWARE E SOFTWARE DELL'AZIENDA CHE PERMETTONO DI MEMORIZZARLI O DI FARLI CIRCOLARE.**

- **IL SISTEMA DELLE INFORMAZIONI RAPPRESENTA QUINDI UN PATRIMONIO ESSENZIALE CHE L'AZIENDA HA NECESSITA' E INTERESSE DI PROTEGGERE.**

- **IMPOSTARE QUINDI UN «METODO» PER INNALZARE IL LIVELLO DI ATTENZIONE RIGUARDANTE IL TRATTAMENTO DEI DATI RITENUTI «CORE» DELL'AZIENDA E/O COMUNQUE RITENUTI RISERVATI, DIVENTA UNA DELLE PRIORITÀ CHE UNA AZIENDA / ORGANIZZAZIONE DEVE AFFRONTARE.**

- **SI DELINEA QUINDI LA NECESSITA' DI AVERE UN SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI «SGSI» O, PER DIRLA ALL'INGLESE «ISMS».**

INFORMATION SECURITY MANAGEMENT SYSTEM

Il Sistema di Gestione della Sicurezza delle Informazioni

UNO SGSI SCHEMATICAMENTE SI PUÒ SPIEGARE NEL SEGUENTE MODO :

- **SISTEMA** ***E' UN METODO DI LAVORO …***
- **GESTIONE**
  … PER ORGANIZZARE LE RISORSE IN PROCESSI E ATTIVITÀ PER …
- **SICUREZZA**
  …GARANTIRE RISERVATEZZA, INTEGRITÀ E DISPONIBILITÀ DELLE…
- **INFORMAZIONI**

(E PRESCINDE DALLE MODALITÀ DI ARCHIVIAZIONE, DAL SUPPORTO IN CUI L'INFORMAZIONE È RIPORTATA. IL SUPPORTO PUÒ ESSERE ELETTRONICO, CARTACEO, ETC.)

TALE SISTEMA VIENE APPLICATO IN UN PERIMETRO DI PROCESSI AZIENDALI, IN BASE A:

- **CRITERI DI RIFERIMENTO AL BUSINESS,**
- **ALL'ORGANIZZAZIONE A PROCESSI,**
- **AI BENI ED ALLA TECNOLOGIA ADOTTATA,**
- **ALLA LOCALIZZAZIONE DELL'ORGANIZZAZIONE.**

Il Sistema di Gestione della Sicurezza delle Informazioni

LA SICUREZZA DELLE INFORMAZIONI PUNTA A CINQUE OBIETTIVI PRINCIPALI :

1. **L' INTEGRITÀ: CIOÈ GARANTIRE CHE I DATI SIANO EFFETTIVAMENTE QUELLI CHE SI PENSANO E NEL DETERMINARE SE I DATI NON SIANO STATI ALTERATI DURANTE LA COMUNICAZIONE (IN MANIERA FORTUITA O INTENZIONALE).**
2. **LA RISERVATEZZA: CHE CONSISTE NELL'ASSICURARE CHE SOLO LE PERSONE AUTORIZZATE ABBIANO ACCESSO ALLE RISORSE SCAMBIATE.**
3. **LA DISPONIBILITÀ: CHE PERMETTE DI MANTENERE IL CORRETTO FUNZIONAMENTO DEL SISTEMA D'INFORMAZIONE E QUINDI GARANTIRE L'ACCESSO AD UN SERVIZIO O A DELLE RISORSE.**

A COROLLARIO:

4. **IL NON RIPUDIO: CHE PERMETTE DI GARANTIRE CHE UNA TRANSAZIONE NON POSSA ESSERE NEGATA.**
5. **L' AUTENTICAZIONE: CHE CONSISTE NELL'ASSICURARE CHE SOLO LE PERSONE AUTORIZZATE ABBIANO ACCESSO ALLE RISORSE, QUINDI NELL'ASSICURARE L'IDENTITÀ DI UN UTENTE, CIOÈ NEL GARANTIRE A CIASCUN CORRISPONDENTE CHE IL SUO PARTNER SIA EFFETTIVAMENTE QUELLO CHE CREDE.**

Il Sistema di Gestione della Sicurezza delle Informazioni

- **LA SICUREZZA DELLE INFORMAZIONI È DIVENTATA UNA SFIDA COMPLESSA E UNA PRIORITÀ IN MOLTE ORGANIZZAZIONI.**

- **NEL TEMPO È STATA UNA RESPONSABILITÀ AFFIDATA E DEMANDATA ALL' IT, MA NEGLI ULTIMI ANNI È UNA TEMATICA CHE COINVOLGE L'INTERO MANAGEMENT AZIENDALE E TUTTI I DIPENDENTI DI UN' AZIENDA.**

- **CAPIRE QUINDI QUALI SIANO I RISCHI (MINACCE, VULNERABILITÀ, IMPATTI) CHE SI HANNO O A CUI SI PUÒ INCORRERE, QUALI SIANO GLI ASSET RITENUTI NEVRALGICI, E QUALI SIANO GLI EVENTUALI PIANI PER GESTIRE INCIDENTI INFORMATICI, SONO INFORMAZIONI IMPORTANTI PER L'AZIENDA COL FINE DI ASSICURARE LA PROPRIA CONTINUITÀ OPERATIVA DEL SERVIZIO VERSO L'ESTERNO (cfr. IATF, ISO 22301).**

- **LA SICUREZZA INFORMATICA, IN QUESTO CONTESTO, CONSISTE NELL'ASSICURARE CHE LE RISORSE HARDWARE E SOFTWARE DI UN'ORGANIZZAZIONE SIANO USATE UNICAMENTE NEI CASI E NEI MODI PREVISTI.**

Il Sistema di Gestione della Sicurezza delle Informazioni

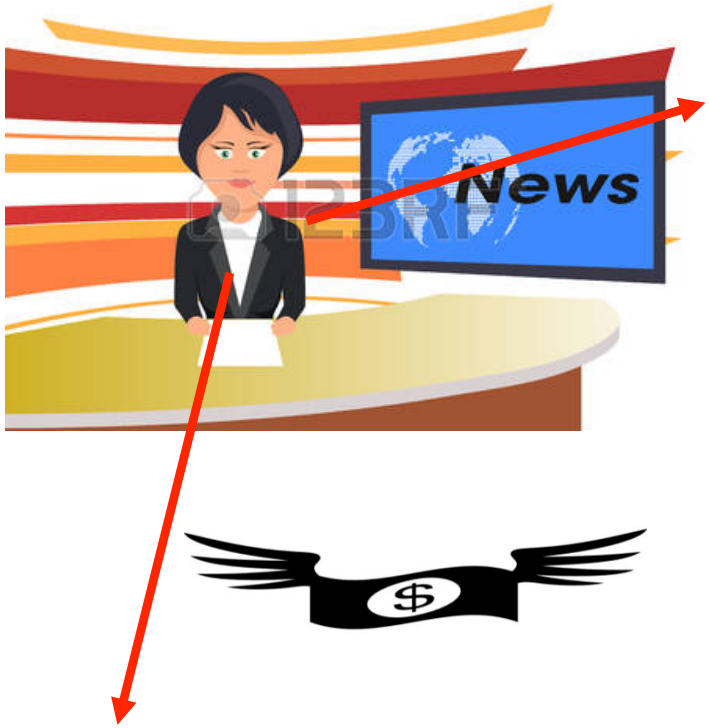
- **LO STANDARD ISO/IEC 27001 È, ATTUALMENTE, L'UNICA NORMA INTERNAZIONALE SOGGETTA A VERIFICA ED ALLA CERTIFICAZIONE CHE DEFINISCE I REQUISITI PER L' ADOZIONE DI UN SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI.**

- **LA NORMA È PROGETTATA PER GARANTIRE LA SELEZIONE DI CONTROLLI DI SICUREZZA ADEGUATI E PROPORZIONATI ALL'ORGANIZZAZIONE AZIENDALE ED AI PROCESSI RIFERITI NELL'AMBITO DELLA CERTIFICAZIONE.**

- **CON L'ADOZIONE DEI CONTROLLI RICHIESTI (114, Annex A), RISULTA QUINDI POSSIBILE PROTEGGERE LE INFORMAZIONI E DARE FIDUCIA AI PROPRI CLIENTI SULL' ACCESSO AL SISTEMA INFORMATICO ED INFORMATIVO AZIENDALE ED AL TRATTAMENTO DEI DATI AZIENDALI.**

- **LA NORMA INDICA UN APPROCCIO PER COSTITUIRE, ATTUARE, APPLICARE, CONTROLLARE, RIESAMINARE, GESTIRE E MIGLIORARE IL SGSI IN OTTICA DI INNALZAMENTO DEL LIVELLO DI SICUREZZA INFORMATICO E DEI DATI RELATIVI ALLA PRIVACY.**

La Sicurezza delle Informazioni: notizie dal web



Uno studio tedesco sul crimine elettronico dimostra che, nel complesso, è aumentata la consapevolezza dei rischi provenienti da internet: l'89% dei dirigenti riconosce per le imprese un rischio alto o molto alto di diventare vittime di tali attacchi, ma solo il 39% di loro considera la propria azienda in pericolo. Di conseguenza, molti non adottano misure di protezione dai rischi virtuali: il 71% delle aziende non dispone di linee guida sulla sicurezza informatica e solo il 17% ha un sistema di gestione IT certificato. Eppure, la sicurezza informatica ha un valore economico enorme: basti pensare che nel 2025 il Digitale creerà globalmente un valore aggiunto di 3,7 miliardi di dollari...

Alcuni esperti affermano che non è possibile raggiungere un livello di sicurezza pari al 100%, ma complicando la vita agli hacker aumenta la probabilità che si riduca la frequenza di tali azioni e quindi anche il rischio per le imprese: bisogna pensare a raggiungere la massima protezione possibile e l'unico modo per farlo è analizzare la sicurezza a fondo e di continuo, in qualunque azienda : **"La cybersecurity è come l'influenza: è impossibile debellarla, l'obiettivo dev'essere ammalarsi di meno e meno frequentemente".**

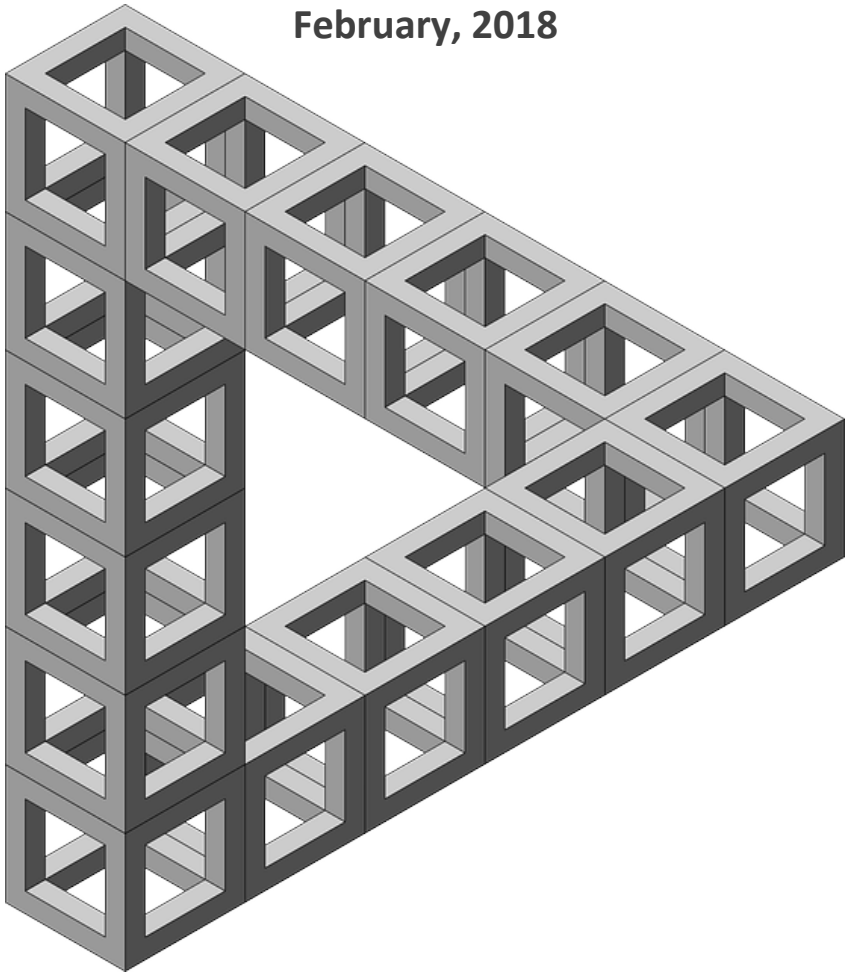
Il Sistema di Gestione della Sicurezza delle Informazioni

...adesso arriva la parte interessante....

VEHICLE INFORMATION SECURITY

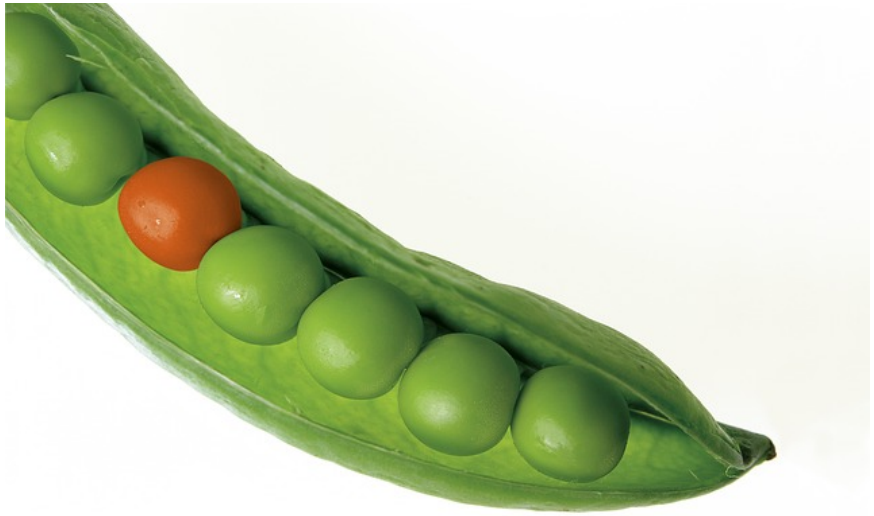
FROM AN UNUSUAL PERSPECTIVE

February, 2018



The unusual speaker

- OpenSource and Community enthusiast
- CEO of two small enterprises:
  - One in Belgium, in the InfoSec domain
  - One in Italy, in the IoT domain



- Why am I here if I don't work on vehicles?
  - Maybe Vehicle InfoSec is not that different from IoT InfoSec...

Vehicle InfoSec and IoT InfoSec

Some similarities between an IoT home network and a private Vehicle network:

- **In both IoT and Vehicles, one of the main cybersecurity issue is the owner (whose only fault is not being an IT expert), e.g. owner introduces a third party inexpensive device with connectivity that creates a hole in the whole network**

- **In both IoT and Vehicles**
  the network is highly heterogeneous

And some differences:

- **IoT vulnerabilities are scary**
  (e.g. wifi baby monitor)
  but not as much as Vehicle vulnerabilities

- **A car could have 100 ECUs and therefore a massive attack surface**

Vehicle InfoSec key points derived from IoT InfoSec (1)

NOTE: A lot of security aspects are not covered by this presentation e.g. Risk Management, InfoSec in Software Development Life Cycle, Technical aspects

Some InfoSec Key Points:

- **Risk assessment for all services and cloud providers and of course Supply Chain InfoSec [first part of this presentation]**
- **Highlight devices which meet InfoSec standards to help consumers choose**
- **Privacy Privacy Privacy (see also GDPR), for example:**
  - **Ability to reset vehicle to factory settings**
  - **Protect personal data from corporations**
  - **Upon request delete personal data also from backend services**

Vehicle InfoSec key points derived from IoT InfoSec (2)

Other InfoSec Key Points:

- **Promptly notify users of threats and actions required**
- **Coordinated vulnerability disclosure (Transparency is key)**
- **Security commitment duration disclosure and continuity plan (e.g. keep on using the unsupported device but disable connectivity)**
- **A mechanism for automated, safe and long term software and/or firmware updates, patches and revisions**
  - **iPhone 5 has now no security updates, after less than 5 years**

Vehicle InfoSec key points derived from IoT InfoSec (3)

Last InfoSec Key Points:

- **Constantly update the bill of materials including software, firmware, hardware and software libraries**
- **Intrusion Detection as cloud service (monitoring, alerting, self-checks)**
- **For administrative access use unique passwords for each vehicle**

Conclusions

How to avoid the digital disaster in the connected world?

Legislation is too slow to be effective.

In my opinion the only way out is a multi-stakeholder effort to adopt self-regulatory frameworks: working together to improve security and privacy in the connected world.