CLOUD COMPUTING AND CYBERSECURITY

Ing. Marcello Miani

- MEMBRO DELLA COMMISSIONE SICUREZZA SUL LAVORO E DELLA COMMISSIONE SICUREZZA CANTIERI DELL'ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI MILANO (OIM)
- MEMBRO GDL «SICUREZZA I4.0»

10/09/2021

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI MILANO

CONSIGLIO NAZIONALE DEGLI INGEGNERI

CLOUD COMPUTING

1. PREMESSA: LE TECNOLOGIE DELL'INDUSTRIA 4.0

- L'INDUSTRIA 4.0 FA RIFERIMENTO ALL'ADOZIONE CONGIUNTA DI TECNOLOGIE DIGITALI IN GRADO DI AUMENTARE L'INTERCONNESSIONE E LA COOPERAZIONE DELLE RISORSE PRESENTI LUNGO LA CATENA DEL VALORE

INDUSTRIA 4.0

- SECONDO MC-KINSEY, L'INDUSTRIA 4.0 SI DECLINA LUNGO 4 DIRETTRICI DI SVILUPPO, SULLE QUALI INVESTIRE :

- 1. DATI, POTENZA DI CALCOLO E CONNETTIVITA' DIFFUSA:
  - Internet of Things, Big data, Machine to Machine communication, Cloud computing

- 2. ANALYTICS AND INTELLIGENCE
  - Digitalizzazione e automazione del lavoro
  - Advanced Analytics

LE DIRETTRICI 1 E 2 RAPPRESENTANO IL MONDO DELLE TECNOLOGIE DELL'INFORMAZIONE (IT)

INDUSTRIA 4.0 – Cont.

* 3. INTERAZIONI UOMO-MACCHINA:

  Interfacce di tipo “ Touch “, Realta’ virtuale ed aumentata

- 4. INTEGRAZIONE COL MONDO FISICO:

  Stampa 3D e manifattura additiva, robotica avanzata (collaborazione uomo-macchina)

LE DIRETTRICI 3 E 4 RAPPRESENTANO IL MONDO DELLE TECNOLOGIE OPERATIVE (OT)

2. LE PROSPETTIVE DELL'INDUSTRIA 4.0

L'INDUSTRIA 4.0 HA LE PROPRIE RADICI NELL'INTEGRAZIONE E CONNESSIONE DI TUTTI GLI ELEMENTI DI UN PROCESSO PRODUTTIVO.

L'INTEGRAZIONE DELLE INFORMAZIONI PUO' ESTENDERSI ALL' ESTERNO CON LE REALTA' DEL PROCESSO DISTRIBUTIVO (MAGAZZINI, TRASPORTATORI, FORNITORI E CLIENTI).

LE PROSPETTIVE DELL'INDUSTRIA 4.0 – CONT.

SARA' PURE POSSIBILE ATTIVARE IL DIALOGO AUTOMATICO TRA SISTEMI, MACCHINARI E ATTREZZATURE, ARRIVANDO ANCHE A CONNETTERE STABILIMENTI GEOGRAFICAMENTE DISPERSI, IN UN' OTTICA DI " COLLABORATIVE MANUFACTURING "

.

QUESTA APERTURA RIVOLUZIONARIA COINVOLGE NUMEROSE TECNOLOGIE, CONSOLIDATE E/O IN VIA DI SVILUPPO

3. DEFINIZIONE DI CLOUD COMPUTING :

- SI DEFINISCE COSI' L'EROGAZIONE DI SERVIZI INFORMATICI

  OFFERTI " ON DEMAND " DA UN FORNITORE AD UN CLIENTE

  FINALE ATTRAVERSO LA RETE INTERNET, A PARTIRE DA UN

  INSIEME DI RISORSE PREESISTENTI, CONFIGURABILI E

  DISPONIBILI IN REMOTO, SOTTO FORMA DI ARCHITETTURA

  DISTRIBUITA

4. IL RUOLO DEL CLOUD NELL'INDUSTRIA 4.0

GRAZIE AL CLOUD L'INTELLIGENZA TECNOLOGICA DIVENTA SEMPRE PIU' PERVASIVA.

IL CLOUD RAPPRESENTA DI FATTO IL TESSUTO CONNETTIVO DELL'INDUSTRIA 4.0.

IL CLOUD SI CONFIGURA COME L'ACCELERATORE DELLA DIGITAL TRANSFORMATION DELLE AZIENDE MANIFATTURIERE, GARANTENDO MAGGIOR FLESSIBILITA' E VELOCITA' DI RISPOSTA ALLE ESIGENZE DEL MERCATO.

IL RUOLO DEL CLOUD NELL'INDUSTRIA 4.0 – CONT.

* LA POTENZA ELABORATIVA, GRAZIE AL CLOUD COMPUTING, E' DISPONIBILE ON DEMAND E IN MODALITA' PAY-PER-USE.

- ESSA SI UNISCE A CONNESSIONI SEMPRE PIU' AFFIDABILI E SICURE, ALLA DIFFUSIONE SEMPRE PIU' CAPILLARE DELLA SENSORISTICA AVANZATA , E AD APPLICAZIONI DI ULTIMA GENERAZIONE, QUALI AD ES. LA REALTA' AUMENTATA.

5. ARCHITETTURA

- L'ARCHITETTURA INFORMATICA DEL CLOUD COMPUTING

  PREVEDE UNO O PIU' SERVER REALI, GENERALMENTE IN FORMA DI SERVER CLUSTER PER MAGGIORE AFFIDABILITA,'

  E FISICAMENTE UBICATI PRESSO IL DATA CENTER DEL FORNITORE DEL SERVIZIO.

- IL CLIENTE UTILIZZA DELLE INTERFACCE MESSE A DISPOSIZIONE DAL FORNITORE PER SELEZIONARE IL SERVIZIO RICHIESTO (AD ES. UN SERVER VIRTUALE COMPLETO OPPURE SOLO STORAGE) E PER AMMINISTRARLO (CONFIGURAZIONE, ATTIVAZIONE, DISATTIVAZIONE)

6. I 5 PRINCIPALI VANTAGGI DEL CLOUD COMPUTING

- FLESSIBILITA’
- ASSENZA DI COSTI FISSI RELATIVI ALL’HARDWARE
- COLLABORAZIONE
- BACK – UP/DISASTER RECOVERY
- SOSTENIBILITA’

7. SVANTAGGI E RISCHI DEL CLOUD COMPUTING

- 1. DOWNTIME

IL DOWNTIME E' SPESSO CITATO COME UNO DEI MAGGIORI SVANTAGGI DEL CLOUD COMPUTING

POICHE' I SISTEMI CLOUD SONO BASATI SU INTERNET, CADUTE DI SERVIZIO SONO SEMPRE UNA SFORTUNATA POSSIBILITA' E POSSONO CAPITARE PER QUALSIASI RAGIONE.

NEL 2017 UN FUORI SERVIZIO DI AMAZON WEB SERVICES COSTO' ALLE VARIE SOCIETA' COINVOLTE FINO A 150 MIO. DOLLARI

DOWNTIME – CONT.

- BEST PRACTICES PER CONTRASTARE IL RISCHIO DOWNTIME

  * PRENDERE IN CONSIDERAZIONE MULTI-REGION DEPLOYMENTS, COME AD ES. AZURE, CHE HA DISTRIBUITO I SUOI SERVIZI DI GESTIONE API (APPLICATION PROGRAMMING INTERFACE) SU PIU' AREE DI AZURE, CON FAILOVER AUTOMATICO PER ASSICURARE LA MASSIMA CONTINUITA' POSSIBILE AL BUSINESS

  * IL FAILOVER AUTOMATICO E' LA TECNICA CHE PREVEDE LA COMMUTAZIONE AUTOMATICA , IN CASO DI GUASTO DI UN ELEMENTO HARDWARE O DI UNA RETE, AD UNA STRUTTURA ANALOGA RIDONDANTE O IN STAND-BY.

RISCHI DEL CLOUD COMPUTING – CONT.

2. SECURITY AND PRIVACY

- OGNI DECISIONE CHE RIGUARDA I DATI DEVE SEMPRE CONSIDERARE ATTENTAMENTE GLI ASPETTI DELLA SICUREZZA (SECURITY) E DELLA PRIVATEZZA (PRIVACY), SPECIALMENTE SE SI TRATTA DI DATI SENSIBILI.

- QUANDO SI MEMORIZZANO DATI E FILES IMPORTANTI PRESSO SERVICE PROVIDERS ESTERNI, CI SI ESPONE SEMPRE A RISCHI, LA CUI PROBABILITA' DI ACCADIMENTO E LA CUI GRAVITA', SE VERIFICATESI, POSSONO AVERE ENORMI CONSEGUENZE.

CLOUD SECURITY – CONT.

- NATURALMENTE SI SUPPONE CHE OGNI CLOUD SERVICE PROVIDER GESTISCA AL MEGLIO E CON OGNI ATTENZIONE ALLA SECURITY L'HARDWARE E LE INFRASTRUTTURE HW E SW MESSE A DISPOSIZIONE DEI CLIENTI.

- TUTTAVIA LA RESPONSABILITA' DELL'UTENTE STA NEL CAMPO DELL'USER ACCESS MANAGEMENT, E STA INTERAMENTE IN LUI LA RESPONSABILITA' DI VALUTARE ATTENTAMENTE TUTTI GLI SCENARI DI RISCHIO.

- PERALTRO, PASSI SONO STATI FATTI PER ASSICURARE LA SICUREZZA E L'INTEGRITA' DEI DATI.

CLOUD SECURITY – CONT.

- UN ESEMPIO E' DATO DALLA GDPR (GENERAL DATA PROTECTION RULE), RECENTEMENTE EMANATA DALLA U.E. PER FORNIRE AGLI UTENTI UN MAGGIOR CONTROLLO SUI LORO DATI
- NEL MAGGIO 2016 E' STATO POI EMANATO IL REGOLAMENTO DELL'U.E. N.2018/679, DIRETTAMENTE APPLICABILE SENZA NECESSITA' DI UNA LEGGE. QUESTO REGOLAMENTO (UN CENTINAIO DI PAG..) DEVE ESSERE SEGUITO DA CHI UTILIZZA DATI PERSONALI E SENSIBILI, E PREVEDE SANZIONI PER CHI LO VIOLA

- TUTTAVIA, E' SEMPRE L'UTENTE CHE DEVE ESSERE CONSCIO DELLE PROPRIE RESPONSABILITA' E SEGUIRE LE BEST PRACTICES

BEST PRACTICES PER MINIMIZZARE I RISCHI DI SECURITY E PRIVACY

* COMPRENDERE IL MODELLO DI RESPONSABILITA' CONDIVISA DEL CLOUD PROVIDER PRESCELTO

- METTERE IN ATTO TUTTI I DETTAMI DELLA SECURITY AD OGNI LIVELLO DELL' ATTIVITA' DELL'UTENTE NEL CLOUD

- SAPERE CHI E' PREVISTO ABBIA ACCESSO AD OGNI RISORSA E SERVIZIO E LIMITARE L'ACCESSO AL PIU' BASSO LIVELLO DI PRIVILEGI

VULNERABILITA' AGLI ATTACCHI

- INTRINSECAMENTE, SI POTREBBE CONSIDERARE UN CLOUD PRIVATO COME IL PIU' SICURO IN ASSOLUTO. IN QUANTO LE SUE RISORSE SONO UTILIZZABILI SOLO DA UN DETERMINATO CLIENTE.

- MA MOLTO DIPENDE DAL LIVELLO DI FAMILIARITA' CHE SI HA CON LE TECNOLOGIE DI SICUREZZA DEL CLOUD. POICHE' SONO QUESTE A PROTEGGERE L'INFRASTRUTTURA PRIVATA

- INOLTRE I COSTI GRAVANO TOTALMENTE IN CAPO ALL'ORGANIZZAZIONE DETENTRICE DEL CLOUD PRIVATO

VULNERABILITA' - CONT.

PER BILANCIARE I RISCHI, MA NEL CONTEMPO CONTENERE I COSTI, LA SOLUZIONE OTTIMALE POTREBBE ESSERE QUELLA DI OPTARE PER I CLOUD IBRIDI, SOLUZIONE VERSATILE CHE E' IN GRADO DI COMBINARE PUBBLICO E PRIVATO

MA ANCHE I CLOUD IBRIDI PRESENTANO POTENZIALI DIFFICOLTA'.

INFATTI LA LORO SICUREZZA PUO' RIVELARSI DI GESTIONE PARTICOLARMENTE COMPLESSA, ESSENDO ESTESI SU PIU' SEZIONI DEL CLOUD.

9. HACKERS ALL'ATTACCO IN ITALIA

- ALLA FINE DEL 2018, 500000 CASELLE DI POSTA ELETTRONICA CERTIFICATA SONO STATI VIOLATE IN ITALIA.
- ADESSO GLI HACKERS HANNO IN MANO GLI IDENTIFICATIVI PEC DI 98000 UTENTI, TRA MAGISTRATI, MILITARI E FUNZIONARI DEL CISR (COMITATO MINISTER. PER LA SICUREZZA DELLA REPUBBLICA)
- E' QUESTO IL PIU' GRANDE ATTACCO CIBERNETICO SUBITO DAL NOSTRO SISTEMA DI SICUREZZA.

10. FEATURES DEL CLOUD COMPUTING

- SCALABILITY E SERVIZI ON DEMAND
- INTERFACCIA USER-CENTRICA: LE INTERFACCE CLOUD SONO INDIPENDENTI DAL LUOGO E AD ESSE SI PUO' ACCEDERE TRAMITE INTERFACCE BEN NOTE, COME INTERNET BROWSERS
- QUALITA' DEI SERVIZI (QoS) GARANTITA,IN TERMINI DI HW/CPU , PRESTAZIONI, LARGHEZZA DI BANDA E CAPACITA' DI MEMORIA
- SISTEMA AUTONOMO: I CLOUDS SONO SISTEMI AUTONOMI GESTITI IN MODO TRASPARENTE ALL'UTENTE. TUTTAVIA, SOFTWARE E DATI POSSONO ESSERE AUTOMATICAMENTE RICONFIGURATI E, SECONDO LENECESSITA' DELL'UTENTE, CONSOLIDATI

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI MILANO

CONSIGLIO NAZIONALE DEGLI INGEGNERI

CYBERSECURITY

1. LA SICUREZZA NELL'INDUSTRIA

- IL PROBLEMA DELLA SICUREZZA IN AMBITO INDUSTRIALE NASCE DA 2 DISTINTE ORIGINI:

- 1. INADEGUATEZZA DELLE REALIZZAZIONI, CHE DERIVANO O DA PROGETTI MALE IMPOSTATI, O DA IMPLEMENTAZIONI SCADENTI DI PROGETTI VALIDI.

IN ENTRAMBI I CASI, ALL'ORIGINE NON VI E' ALCUNA

AZIONE INENZIONALMENTE NEGATIVA

LA SICUREZZA NELL'INDUSTRIA – CONT.

- 2. . INTERVENTI MALEVOLI, CHE IMPEDISCONO IL FUNZIONAMENTO CORRETTO E REGOLARE DI IMPIANTI E MACCHINE, COME IPOTIZZATO NEL PROGETTO ED ATTUATO NELLA FASE REALIZZATIVA , SEGUENDO LE BEST PRACTICES AZIENDALI

LA SICUREZZA NELL'INDUSTRIA – CONT.

- QUESTO SECONDO TIPO DI GUASTO E' QUELLO CHE PIU' RAPPRESENTA IL RISCHIO NELL'AMBITO DELLE MODERNE REALTA' INFORMATICHE E DI TELECOMUNICAZIONE, DOVE L'INTERCONNESSIONE DI RETI E SISTEMI CRESCE CONTINUAMENTE

* E QUANDO SI PARLA DI CYBERATTACCHI, CI SI RIFERISCE PROPRIO A QUESTI INTERVENTI MALEVOLI INTENZIONALI

2. CYBERSECURITY E CYBERSAFETY

- QUAL'E' LA DIFFERENZA FRA CYBERSECURITY E CYBERSAFETY?

FACENDO ANCHE RIFERIMENTO A QUANTO DETTO AL PUNTO 1., FONDAMENTALMENTE LA CYBERSAFETY SI FOCALIZZA SULLE PERSONE, MENTRE LA CYBERSECURITY COINVOLGE IL MONDO DELL'INFORMAZIONE.

* TUTTAVIA, QUESTA DISTINZIONE, PER QUANTO SOSTANZIALMENTE VERA, NON E' DEL TUTTO ESAURIENTE

3. IL MONDO E' PIU' CHE MAI INTERCONNESSO

- I PROGRESSI TECNOLOGICI SONO BASATI SU UNA CONNETTIVITA' CRESCENTE
- I NOSTRI DATI SONO CONDIVISI ED UTILIZZATI DA PIU' UTENZE CHE MAI, CON GRAN BENEFICIO PER TUTTI
- MA C'E' UN PREZZO DA PAGARE: PIU' DIVENTIAMO CONNESSI, PIU' I NOSTRI DATI SONO VULNERABILI

4. Cybersecurity Report 2015 – Deutsche Telekom

- PIU' DI UN TERZO DELLE AZIENDE VENGONO SOTTOPOSTE A CYBERATTACCHI ALMENO UNA VOLTA ALLA SETTIMANA

- 9 SU 10 AZIENDE SONO GIA' STATE VITTIME DI UN CYBERATTACCO

5. I TRENDS PIU' IMPORTANTI PER LA CYBERSECURITY NEL 2020

SECONDO L'ECONOMIC FORUM DI DAVOS 2020

* LA CYBER"GUERRA FREDDA" TRA EST ED OVEST E' DESTINATA AD AUMENTARE

- LA RETE 5G E L'INTERNET DELLE COSE (IoT) CONTRIBUISCONO A RENDERCI PIU' VULNERABILI AI CYBERATTACCHI
- LE AZIENDE COMINCERANNO A RIPENSARE IL LORO APPROCCIO AL CLOUD COMPUTING

6. L'INDUSTRIA 4.0

- IL CONCETTO DI INDUSTRIA 4.0 SOTTINTENDE L'INFORMATIZZAZIONE AVANZATA DEI PROCESSI PRODUTTIVI E DELLA LOGISTICA (IN GENERE APPLICAZIONI DI TELEMATICA TRAMITE RETI WIRELESS)
- L'INTEGRAZIONE CON CLIENTI E BUSINESS PARTNERS
- LA BASE TECNOLOGICA E' DATA DAI SISTEMI INFORMATICI E DI TLC, E DALL'IoT

IMPORTANZA PER LE AZIENDE DI I 4.0

- NEL 2014 SOLO AL 38% DELLE AZIENDE ERA CONOSCIUTO IL CONCETTO DI I 4.0
- OGGI SIAMO A PIU' DELL'85%
- IL PIU' GRANDE RISCHIO PER ESSE: UN CYBERATTACCO

7. DUBBI SULLA SICUREZZA DEL CLOUD

- UNA COMPONENTE IMPORTANTE DELL' INDUSTRIA 4.0 E' IL CLOUD COMPUTING.

- L'UTILIZZO DEI SERVIZI CLOUD E' IN CONTINUA CRESCITA, MA QUESTA FORMA DI MEMORIZZAZIONE ESTERNA DEI DATI E DELLE PROCEDURE GENERA SEMPRE PIU' RIFLESSIONI SULLA SICUREZZA.
- IL CYBER SECURITY REPORT DEL 2015 RIPORTA CHE SOLO IL 24% DEGLI ALTI MANAGER RITIENE SICURO IL CLOUD COMPUTING

8. APPROCCIO AZIENDALE AL CLOUD – CONT.

- SOLUZIONI PER LA SECURITY DEVONO EVOLVERE VERSO NUOVE ARCHITETTURE BASATE SUL CLOUD, PIU' FLESSIBILI, E CHE ASSICURINO UN LIVELLO DI PROTEZIONE SCALABILE CON LA VELOCITA' DEI PROCESSI INFORMATICI.
- CRESCE IL RICORSO A CLOUD IBRIDI/PRIVATI

9. LA CYBERSECURITY RIGUARDA ANCHE L'HARDWARE

- LE TECNOLOGIE A SEMICONDUTTORI SONO ESSENZIALI PER L'ODIERNA ECONOMIA E LA PROSPERITA' DI DOMANI

- UNA CYBERSECURITY GLOBALE RICHIEDE CHE INFRASTRUTTURE CRITICHE SIANO PRODOTTE DA SORGENTI PRODUTTIVE DIVERSIFICATE, E CHE I FUTURI PROGRESSI NELL'HARDWARE SIANO GARANTITI IN PIU' SEDI.

10. ATTORI PUBBLICI E PRIVATI: COMPITI E RUOLI

- PER ASSICURARE LA SICUREZZA DELLA NOSTRA INFRASTRUTTURA DIGITALE, E' NECESSARIA LA PARTNERSHIP DEI SETTORI PUBBLICO E PRIVATO

* IN QUESTA PARTNERSHIP IL SETTORE PUBBLICO STABILISCE DEGLI STANDARDS E SVILUPPA CONTROLLI, MENTRE IL SETTORE PRIVATO PROGETTA, COSTRUISCE E PROMUOVE LA REALIZZAZIONE DEI VARI DISPOSITIVI/MACCHINE, IN ACCORDO CON GLI STANDARDS

11. L'EVOLUZIONE DEL RUOLO DEL SETTORE PUBBLICO

- CON L'OBBIETTIVO DI RENDERE IL PAESE PIU' SICURO E RESILIENTE ANCHE NEL DOMINIO DIGITALE, L'ITALIA HA EMANATO UN D.L. (n.82 DEL 14/6/2021), CHE CONTIENE:

* DISPOSIZIONI URGENTI IN MATERIA DI CYBERSICUREZZA

- DEFINIZIONE DELL' ARCHITETTURA NAZIONALE DI CYBERSICUREZZA, E

- L'ISTITUZIONE DELL' AGENZIA PER LA CYBERSICUREZZA NAZIONALE

12. AGENZIA PER LA CYBERSICUREZZA NAZIONALE

- L' ORGANIZZAZIONE ED IL FUNZIONAMENTO DELL' AGENZIA SONO DEFINITI IN UN APPOSITO REGOLAMENTO, IN FASE DI MESSA A PUNTO.

- IL SUDDETTO REGOLAMENTO E' ADOTTATO, ENTRO 120 GIORNI DALLA DATA DI ENTRATA IN VIGORE DELLA LEGGE DI CONVERSIONE DEL PRESENTE DECRETO, CON ALTRO DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

- VA DATO MERITO ALL'ON. DRAGHI DI AVER DATO UNA ACCELERAZIONE DECISIVA NEL CAMPO DEGLI INTERVENTI PUBBLICI PER LA CYBERSICUREZZA

13. ATTACCO HACKER ALLA REGIONE LAZIO

- MA PROPRIO IN QUESTO PERIODO ABBIAMO ASSISTITO AD UN EVENTO CHE DIMOSTRA COME IL MALWARE NON CONOSCE SOSTE E SFIDA GLI INTERVENTI PROGRAMMATI PER LA CYBERSICUREZZA.

- ALLA FINE DI LUGLIO 2021, UN ATTACCO HACKER HA BLOCCATO IL FUNZIONAMENTO DEL SISTEMA DI PRENOTAZIONE VACCINALE ANTI-COVID E DELL' ANAGRAFE VACCINALE DELLA REGIONE LAZIO.

ATTACCO HACKER ALLA REGIONE LAZIO – CONT.

- IL SITO INFORMATICO E' RIMASTO INACCESSIBILE PER CIRCA UNA SETTIMANA, E DAL 5/8 SI STA RIPARTENDO CON UN CRONOPROGRAMMA DEI SERVIZI IN VIA DI RIATTIVAZIONE

- GLI INVESTIGATORI STANNO CERCANDO DI CAPIRE L'ORIGINE DEGLI ATTACCHI E SONO A CACCIA DEGLI INDIRIZZI IP (INTER-NET PROTOCOL ADDRESS) DA CUI SON PARTITI

- FORTUNATAMENTE GLI HACKER HANNO BLOCCATO, CRIPTANDOLI, I SERVER CHE GESTISCONO LE COPIE DEI FILES DI BACK-UP, MA NON HANNO TOCCATO LE COPIE DEI FILES STESSI

ATTACCO HACKER ALLA REGIONE LAZIO – CONT.

- COSI' SI E' POTUTO, CREANDO UN SISTEMA EQUIVALENTE A QUELLO CRIPTATO DAGLI HACKER, ARRIVARE AI FILES DI BACK-UP E RIPARTIRE IN FRETTA
- DETERMINANTE E' STATO IL SUPPORTO FORNITO DA FBI ED EUROPOL, CON CUI LA POLIZIA POSTALE STA ANCORA LAVORANDO
- SI STANNO ANALIZZANDO I DATI, SUI FILES DI LOG ACQUISITI IN QUESTI GIORNI, IN MODO DA CAPIRE DA QUALE PAESE L' AZIONE E' PARTITA
- SEMBRA CHE AGLI HACKER NON SIA STATO PAGATO ALCUN RISCATTO