Linea Amica

LADIDATTICA edizione 2024

FORMAZIONE ONLINE PER LA PA

PROGRAMMA OPERATIVO COMPLEMENTARE

Agenzia per la Coesione Territoriale

Presidenza del Consiglio dei Ministri
Dipartimento della Funzione Pubblica

FORMEZ
AL SERVIZIO DELLA PA

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

Ciclo di Webinar

Rivoluzione digitale: le nuove sfide per la PA tra PNRR, Cybersecurity e Intelligenza Artificiale

PROGRAMMA OPERATIVO COMPLEMENTARE

Agenzia per la Coesione Territoriale

Presidenza del Consiglio dei Ministri
Dipartimento della Funzione Pubblica

FORMEZ
AL SERVIZIO DELLA PA

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

Linea Amica

LADIDATTICA
FORMAZIONE ONLINE PER LA PA
edizione 2024

Andrea Tironi
Massimo Poletti

Governance della cybersecurity e autodifesa digitale negli Enti locali

Venerdì 19 aprile 2024

Massimo Poletti

Dirigente Servizio Sistemi Informativi
Responsabile per la Transizione al Digitale

Comune di Ferrara

https://www.linkedin.com/in/massimopoletti

DISCLAIMER: Le informazioni contenute in questa presentazione sono esclusivamente le opinioni personali del relatore e non riflettono necessariamente le posizioni o le vedute del Comune di Ferrara o di altri Enti/Società citati.

E voi chi siete?

- In tanti pensano che non saranno mai oggetto di un incidente di sicurezza
- Moltissime persone e aziende in fondo lo sanno ma ignorano il problema (un po' come certe malattie, non faccio prevenzione e spero capiti a qualcun altro)

UN PASSO INDIETRO: LA STORIA RECENTE DELL'INFRASTRUTTURA INFORMATICA DEL COMUNE DI FERRARA

2019:

- Dominio AD 2008, tanti PC con Windows XP e 7 (su un totale di circa 800 postazioni), molti server pre-Windows Server 2012
- Risorse applicative prevalentemente on-premise (server fisici + server farm virtualizzata) rispetto al cloud (50% interno, 20% cloud ibrido presso in house Lepida, 30% SaaS)
- File server: presente nel datacenter interno, ma soprattutto molti NAS sparsi tra i servizi
- Sicurezza: Antivirus, Firewall, VPN attestate al firewall (no 2FA), accesso remoto con strumenti generici vari

Evoluzione 2019-2023:

- Migrazione a AD 2016, eliminazione Windows XP, riduzione Windows 7, riduzione Windows Server < 2012
- Noleggio di 2 blade e predisposizione ambiente virtualizzato presso Lepida
- Migrazione/sostituzione/aggiornamento applicativi: 10% interno, 40% cloud ibrido, 50% SaaS
- File server: creazione di NAS virtuali presso Lepida al fine di eliminare i NAS e i file server interni; al momento dell'incidente il processo di migrazione era iniziato da circa un mese
- Sicurezza: quanto elencato sopra, più modulo Forticlient per i portatili (acquistato durante il periodo di smart working)

VI RICONOSCETE?

Tutto ciò è ovviamente insufficiente, e infatti c'era pronto per il 2024 il progetto per una piattaforma specifica e i servizi SOC.

CE L'AVEVAMO QUASI FATTA! E INVECE…

12 LUGLIO 2023

Postazioni informatiche e numero verde 800.532532 temporaneamente inattivi. Tecnici e operatori comunali al lavoro per risolvere la situazione

Attacco hacker alla rete internet del Comune, disabilitati per sicurezza i servizi

DI COSA PARLEREMO

- Isolamento e contenimento; valutazione dell'impatto
- Organizzazione delle fasi di risposta e ripristino
- Ripristino dell'infrastruttura, delle postazioni di lavoro e dei servizi
- Recupero dei dati
- Gestione del rapporto con il Garante (pubblicazione dei dati)
- Lezione appresa e sviluppi futuri


Non lasciare che una
buona crisi vada sprecata!


Come prepararsi
all'apocalisse?


KEEP
CALM
AND
MAKE YOUR
CALLS

OPERAZIONI DA FARE IMMEDIATAMENTE

DAL PUNTO DI VISTA TECNICO (isolamento e contenimento):

- **Disconnettere** l'Ente da tutti i collegamenti esterni (internet, VPN, enti terzi, ecc.) senza spegnere gli apparati, specialmente i Firewall
- **Disconnettere** dalla rete LAN tutti i dispositivi:
  - Server e NAS senza spegnerli
  - PC o dove sono presenti PC embedded (es. totem), possibilmente senza spegnerli
  - Fortemente consigliato lo spegnimento delle stampanti di rete
  - Per gli AP e i dispositivi IoT (tra i quali metto anche i marcatempo) vedere se si possono isolare le rispettive VLAN (ci sono?)
- **Attendere** il Response Team (fatta la telefonata?) che ovviamente non può collegarsi da remoto

DAL PUNTO DI VISTA ORGANIZZATIVO:

- **Stabilire** subito (o nel più breve tempo possibile) un paio di ruoli fondamentali:
  - Chi si occupa di organizzare la parte tecnica
  - Chi si occupa della parte gestionale-organizzativa e terrà i rapporti con il top management/parte politica ed eventualmente con l'esterno

  ammesso che i ruoli possano essere separati, ma sarebbe un grosso disagio se ciò non fosse possibile in quanto i tecnici IT (interni e esterni) devono essere protetti da pressioni che possono arrivare dall'Ente ed eventualmente dai cittadini

AZIONI DI TIPO ORGANIZZATIVO – LE PRIME COSE DA FARE

- **Avvisare immediatamente i vertici dell'Ente** Direttore Generale, Sindaco, Segretario, Dirigenti Apicali (telefono), Dirigente delegato Privacy o Privacy Officer (se nominati)
- **Avvisare subito dopo tutti i Dirigenti e le E.Q.** (messaggi, telefono, posta elettronica)
- **Avvisare** per posta elettronica tutti i **dipendenti e collaboratori**
- **Avvisare il Responsabile per la Protezione dei Dati (RPD-DPO)**
- Fare diffondere subito un primo **comunicato stampa** per avere il controllo su quello che leggeranno i cittadini (lo sanno già che è successo qualcosa)
- **Organizzare** un comitato di crisi in modo che ci si possa sempre confrontare in pochi. Serve comunque un forte commitment e **una grande fiducia** nei confronti di chi sta gestendo la crisi da parte dei vertici dell'Ente. Devono fidarsi di quanto viene consigliato loro di fare.
- Nella comunicazione (specialmente quella interna) **mantenere un tono tranquillo**, di chi sa perfettamente cosa fare; dare delle **chiare disposizioni** e fare capire che devono essere rispettate; reiterare le comunicazioni interne ogni qual volta ci siano novità che si riflettono sul lavoro, quelle esterne quando si ritiene di evidenziare a cittadini e utenti i tempi di ripristino dei servizi.

AZIONI DI TIPO ORGANIZZATIVO – COMUNICAZIONI

- **Polizia Postale:** in giornata, massimo giorno dopo
- **Garante per la protezione dei Dati Personali:** entro 72 ore (concordare cosa scrivere con RPD-DPO) segnalazione preliminare
- **ACN**: quando la situazione dal punto di vista tecnico è un po' più chiara a seguito delle prime attività svolte dal Response Team (tre-quattro giorni?). ATTENZIONE: prossime novità normative (DDL Cybersicurezza)
- Per Polizia Postale e Garante occorre avere titolo (essere legale rappresentante o avere una delega) per presentare la denuncia, per ACN tipicamente segnala il responsabile IT

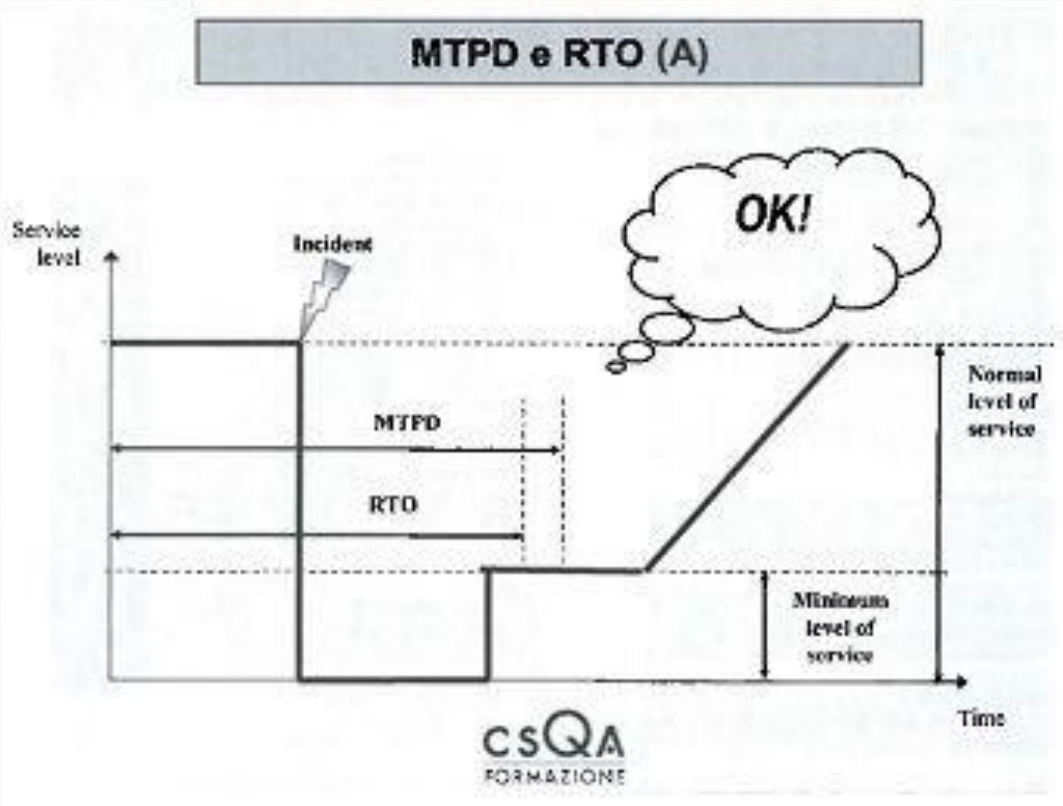
MISURA TECNICA - INVENTARIO DI CIÒ CHE È STATO O POTREBBE ESSERE STATO COMPROMESSO (valutazione dell'impatto)

- Insieme al Response Team occorre **fare un inventario** di ciò che è stato cifrato, di ciò che è stato sicuramente compromesso e di ciò che potrebbe esserlo stato.
- Fin da questa prima fase occorre la collaborazione dei sistemisti interni (se esistono) e/o del supporto di chi fornisce i servizi sistemistici al lavoro del Response Team
- Da attenzionare i Domain Controller, le server farm virtualizzate, i backup, le piattaforme di infrastruttura quali antivirus, ecc.
- Controllare gli applicativi in SaaS puro che teoricamente sono quelli meno esposti rispetto ad un attacco nella nostra infrastruttura. **TUTTO CIÒ CHE ERA IN CLOUD (SAAS O IBRIDO) NON È STATO COINVOLTO**, quindi posta elettronica, sportelli telematici di front office e principali applicativi gestionali.
- Verificare la situazione a livello postazioni di lavoro (spente o accese durante l'attacco)
- Verificare come attivare delle connessioni sicure per gli interventi dei fornitori

PILLOLA DI BUSINESS CONTINUITY

- Due punti critici sono RTO (tempo entro il quale deve essere ripristinato un servizio) e MTPD (massimo periodo tollerabile di interruzione del servizio)
- Il CONSIGLIO che posso dare è di tenere un inventario il più possibile esaustivo e documentato di tutte le procedure, grandi e piccole, locali e in cloud, che sono in produzione e permettono lo svolgimento delle attività dell'Ente. Individuarne la reale criticità.
- Faccio l'esempio del "mandato informatico", è una piccola procedura su un piccolo server che permette di trasmettere al tesoriere i mandati per gli stipendi e la liquidazione delle fatture. Niente di che, ma senza quella non si paga.
- Quindi, nel nostro caso, la prima criticità è stata individuata nell'elaborazione degli stipendi e nel relativo pagamento:

- PC portatili di emergenza per il Servizio del Personale collegati a Internet tramite WiFi pubblico EmiliaRomagnaWiFi
- VPN per connettersi direttamente dall'esterno al gestionale presso il datacenter di Lepida
- Ripristino del server "mandato informatico"

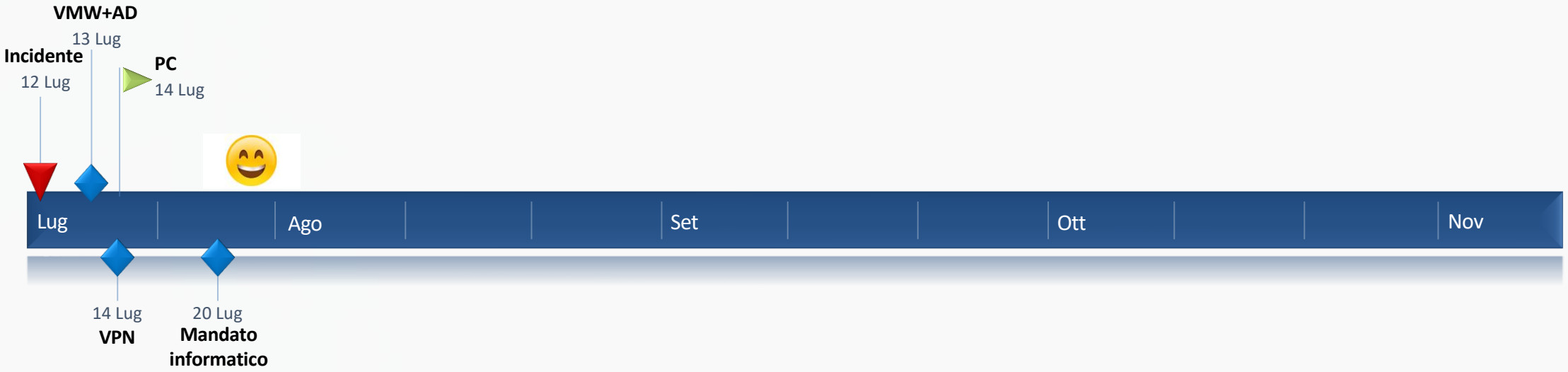


- Fare un **inventario** dello stato dei servizi, suddividendo i servizi di front office (a massima visibilità) da quelli di backoffice, quelli che servono a erogare prestazioni verso l'esterno da quelli puramente funzionali all'operatività dell'ente
- Individuare i **servizi critici** interrotti sui quali concentrare lo sforzo per un celere ripristino. Es: erogazione stipendi.
- **Condividere** le scelte nell'ambito del comitato di crisi, ma comunque in questa fase agire in fretta, anche con giri di telefonate o rapide video call.

Un'utilissima misura preventiva, ripeto, è quella di avere un inventario aggiornato di tutte le procedure in uso, collegando ognuna alle risorse utilizzate per il loro funzionamento (hardware, software, supporto del fornitore, referenti interni, ecc.) e ai servizi che tengono in piedi, basta un foglio Excel. Si rivelerà molto utile in casi come questo.

Questa, tra l'altro, è una misura minima di sicurezza prevista dalla circolare AGID n. 2/2017.

IL SERVIZIO PIÙ CRITICO: GLI STIPENDI



- **12 luglio (mercoledì):** incidente
- **13 luglio (giovedì):** creata nuova infrastruttura AD e VMWare (in datacenter Lepida)
- **14 luglio (venerdì)**: create da parte di Lepida le VPN per l'accesso diretto al gestionale da parte del personale dell'Ente e da quello del service paghe; inizio della preparazione dei PC portatili disponibili in magazzino per il Servizio del Personale
- **17 luglio (lunedì):** personale interno e del service sono in grado di lavorare sull'elaborazione stipendi
- **20 luglio (giovedì):** ripristinato server mandato informatico e conseguente invio, nei giorni seguenti, dei mandati al tesoriere
- **26 luglio:** stipendi pagati regolarmente

MISURA TECNICA – RISTRUTTURARE O RICOSTRUIRE?

Una scelta della massima importanza è quella tra cercare di recuperare l'infrastruttura di dominio o ricostruirla da zero:

RECUPERARE

PRO: sostanziale accorciamento dei tempi, costi ridotti o nulli

CONTRO: nessuna totale sicurezza sulla presenza di persistenze, probabili residui di utenze e policy non sicure, mancata sostituzione di postazioni obsolete

RICOSTRUIRE

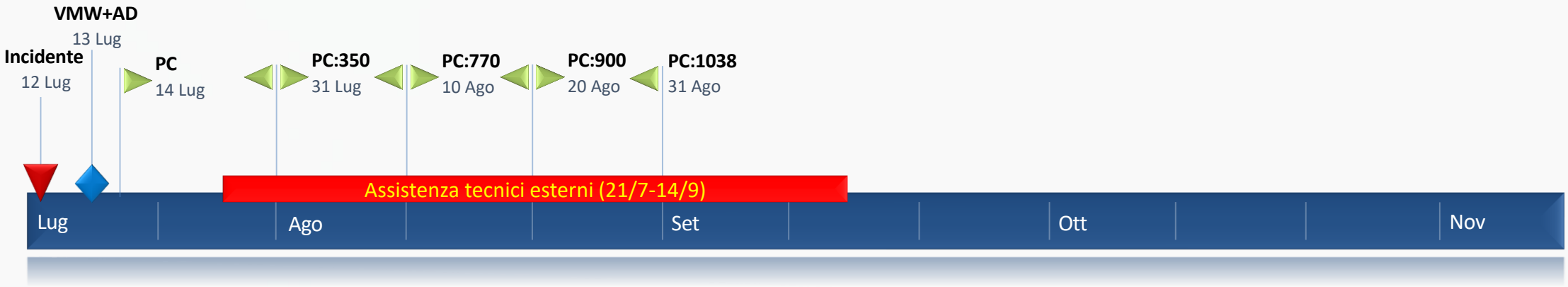
PRO: nuova infrastruttura pulita, possibilità di impostare un hardening efficace, occasione per eliminare gli apparati obsoleti

CONTRO: tempi e costi per ripassare tutte le postazioni di lavoro dell'ente ed eventualmente sostituirle

IN AMBO I CASI: ci saranno probabilmente licenze di prodotti di sicurezza da acquisire

MISURA ORGANIZZATIVA: LA MANODOPERA ESTERNA

- Al 31 luglio con le risorse interne (compresa la ditta che ha in appalto la manutenzione delle PdL) erano state ripristinate circa 350 postazioni di lavoro, comprendendo sia PC nuovi che avevamo a magazzino (installabili in fretta) sia un certo numero di PC revisionati (i più "facili") con le modalità illustrate nel diagramma di flusso.
- Era chiaro che non avremmo potuto farcela con le nostre forze, tenendo conto sia che c'erano parecchie situazioni complicate dal punto di vista logistico, nonché della numerosità delle sedi. Inoltre nel corso del mese di agosto abbiamo reperito da fornitori locali circa 60 portatili e 40 desktop.
- È iniziata una ricerca di tecnici disponibili presso diverse realtà locali e presso la in house Lepida, ricerca resa difficile dal particolare periodo in cui i tecnici di sarebbero serviti, ovvero il mese di agosto.
- Un grandissimo aiuto è stato fornito dall'Università degli Studi di Ferrara, con la quale abbiamo un ottimo rapporto e numerose collaborazioni in diversi campi, ad esempio quella con il CERVAP (Centro di Ricerca sul Valore Pubblico). I colleghi che gestiscono il team di tecnici interni ci hanno offerto la disponibilità di numerose unità di personale che durante il mese di agosto sarebbero state presenti in servizio ma con scarsi carichi di lavoro per la sospensione dell'attività didattica.
- TECNICI UNIFE: 82 gg/uomo a titolo gratuito TECNICI DITTE ESTERNE + LEPIDA a pagamento: 53 gg/uomo



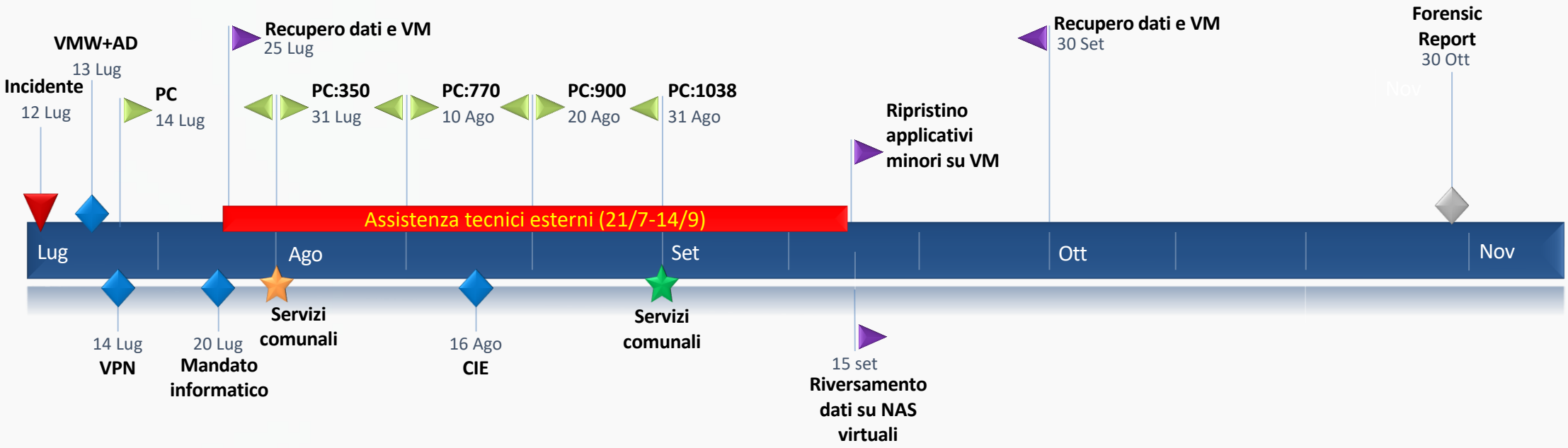
IL RECUPERO DEI DATI

QUALI DATI SONO STATI CIFRATI E QUALI NO

- **CIFRATI:** dati residenti su macchine a Dominio (DC, File Server, NAS, PC), dati in procedure su VM o macchina fisica in datacenter comunale (VM cifrate)
- **NON CIFRATI:** dati residenti su sistemi in cloud (SaaS puro e SaaS ibrido), dati residenti su macchine e PC spenti al momento dell'attacco (esisteva direttiva di spegnimento notturno dei PC), dati residenti su macchine e NAS non a dominio e senza condivisioni attive al momento dell'attacco
- **La grande quantità di dati cifrati ha creato enormi difficoltà a molti Servizi dell'Amministrazione**
- **Premesso che non è stata presa in considerazione l'opzione di pagare il riscatto,** sono state percorse due strade:
  - **Da parte nostra** la ricerca sul mercato di società specializzate che potessero provare a decifrare: **sì, esistono**
  - **Da parte di ACN** l'analisi della situazione per verificare se esistessero metodi di recupero applicabili: **sì, esistevano**

AGGIORNAMENTO TIMELINE

- Stazioni di lavoro: il 31 agosto abbiamo chiuso il laboratorio; il totale delle postazioni di lavoro preparate è 1038, il numero di utenti creati nel nuovo dominio è 1007. L'installazione presso le sedi degli utenti è terminata a metà settembre.
- Stato servizi comunali: al 31 luglio tutti i servizi di front office attivi (salvo CIE), al 31 agosto attivi anche tutti i relativi servizi di backoffice; CIE ripristinate dal 16 agosto in quanto occorreva attendere le nuove macchine dal Ministero.
- Recupero dati: iniziato il 25 luglio, terminato il 30 settembre.
- NOTA BENE: il recupero dei dati e il loro riversamento sui NAS virtuali implica un loro preventivo esame con antivirus e altri strumenti di analisi. Il recupero delle VM non vuol dire che verranno rimesse in linea così come sono, in quanto ci potrebbero essere delle persistenze. Quindi da esse si recuperano e si verificano i dati, si creano VM nuove, si reinstallano gli applicativi e si importano i dati. Tutto ciò quando esiste ancora il fornitore, in caso contrario emergono criticità da gestire.



ANALISI FORENSE

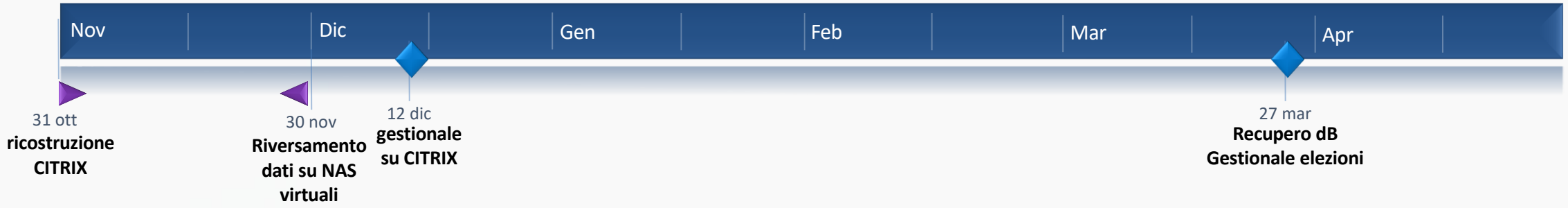
- Il Response Team ha potuto analizzare durante la sua attività, molto intensa i primi momenti poi successivamente scemata per lasciare posto a quella dell'assistenza sistemistica, tutti i materiali che ha avuto a disposizione. Purtroppo il firewall è stato spento bruscamente con conseguente perdita dei log. Comunque hanno avuto a disposizione diversi sistemi da analizzare, in particolare un server dove la cifratura è stata interrotta e quindi l'eseguibile del ransomware era ancora disponibile (Gang Rhysida).

- Sintetizzando molto ciò che è emerso dall'analisi forense, consegnata il 30 ottobre:
  - Non è stato possibile trovare il "paziente zero", anche perché non era possibile tenere fermi tutti i PC compromessi. Tuttavia è stata conservata, ed è tuttora in cassaforte, una copia di molto materiale. La conserveremo per un tempo ragionevole prima di distruggerla.
  - La causa più probabile è stato un phishing aperto da un utente con privilegi di amministratore locale e conseguente installazione di software sul PC, poi da lì movimenti laterali ed escalation di privilegi fino ad arrivare al DC
  - Sono stati trovati e utilizzati vecchi account amministrativi creati molti anni prima per finalità varie
  - La cifratura è partita da alcune stazioni di lavoro, compromesse, che hanno permesso di fare danni in particolare alle condivisioni

- È però importante sottolineare come l'attacco vero e proprio non sia stato sferrato solo con strumenti più o meno automatici. Alcune azioni che sono state svolte implicano una notevole competenza tecnica e l'intervento diretto di un sistemista esperto che ha studiato in profondità il contesto. Ad esempio, l'accesso al portale dell'Antivirus per disabilitarlo, l'accesso al sistema di backup che richiedeva l'utilizzo di una VPN (ahimè, senza 2FA) più delle credenziali utente.

COSA RIMANE DA FARE DAL PUNTO DI VISTA TECNICO

- A partire dal 1° novembre si è partiti con la ricostruzione dell'infrastruttura Citrix, utilizzata primariamente per il lavoro remoto. Il lavoro lo consideriamo terminato nel momento in cui il nostro gestionale principale (Suite Maggioli Sicr@web) è stato raggiungibile (si trova in Cloud ibrido) da remoto via Citrix, il 12 dicembre. NOTA: con il progetto PNRR M1C1 1.2 (migrazione al Cloud) il gestionale Maggioli dai primi di marzo 2024 è raggiungibile direttamente da Internet.
- Il riversamento sui NAS virtuali dei documenti in precedenza sparsi per l'Ente è terminato il 30 novembre.
- Sono tuttora in corso i ripristini di programmi minori, che tuttavia creano reali disagi ad alcuni ristretti gruppi di utenti, pur non causando disservizi per l'utenza esterna. Richiamando il principio di Pareto, lo sforzo per l'ultimo 20% dei lavori è notevole rispetto a quello già sostenuto (sotto un esempio).
- Si sta approfondendo con la società in house Lepida l'adozione di un backup immutabile.



E LA PRIVACY?

- **L'incidente ha richiesto un notevole impegno per la corretta gestione dei rapporti con il Garante. Le figure del DPO, del dirigente delegato Privacy, del dirigente dei Sistemi Informativi nonché RTD e dei comunicatori sono state molto importanti.**
- **IL 20 agosto la gang Rhysida, a fronte del rifiuto di trattare per il pagamento di un riscatto, ha iniziato la pubblicazione (in tre tranche) di circa 1,6 TB di dati. Si è trattato della pubblicazione casuale di cartelle esfiltrate da differenti server e computer.**
- **La pubblicazione ha creato un ulteriore livello di complessità nella gestione del rapporto con il Garante.**


GPDP

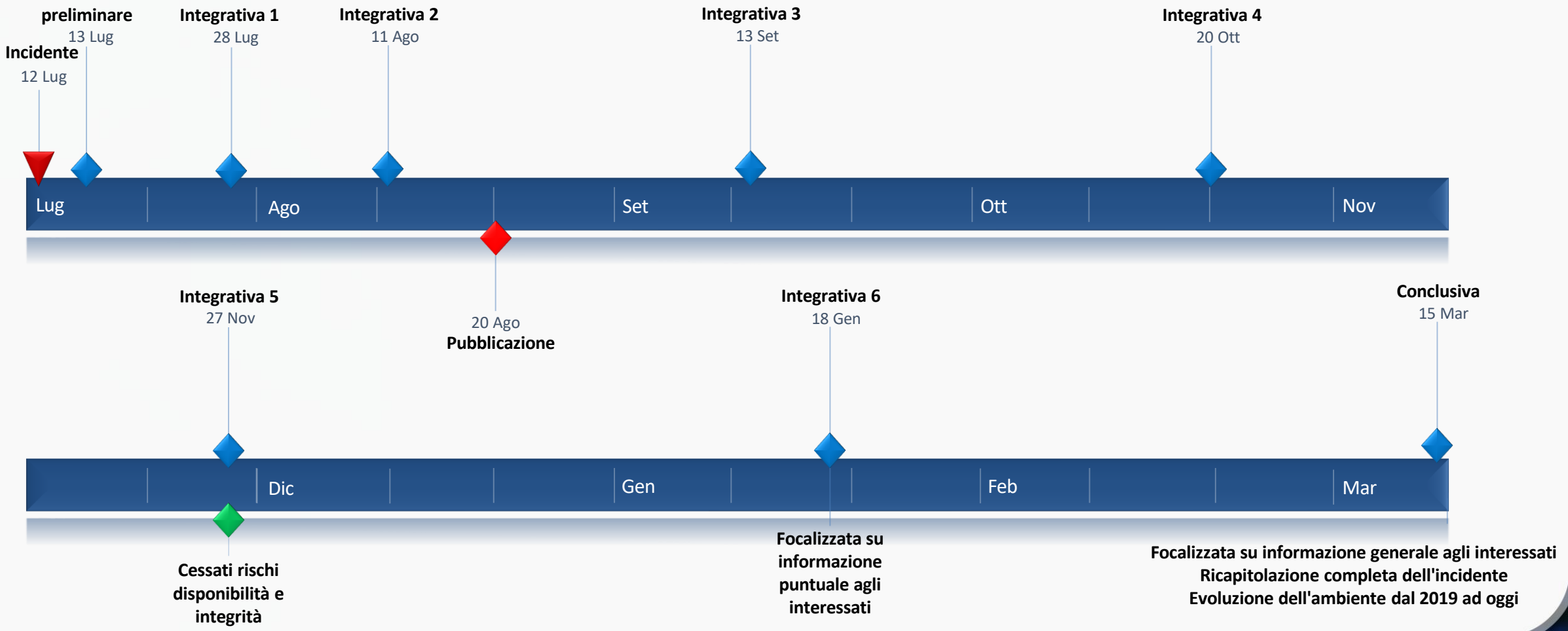
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

21 Agosto 2023

Reso noto per ora il 33% delle informazioni. Il rilascio, come comunicato dal gruppo criminale informatico, sarà graduale. Ecco cosa è stato pubblicato

Attacco informatico al Comune di Ferrara, i primi dati 'hackerati' già online

TIMELINE RAPPORTO CON IL GARANTE



RICAPITOLANDO

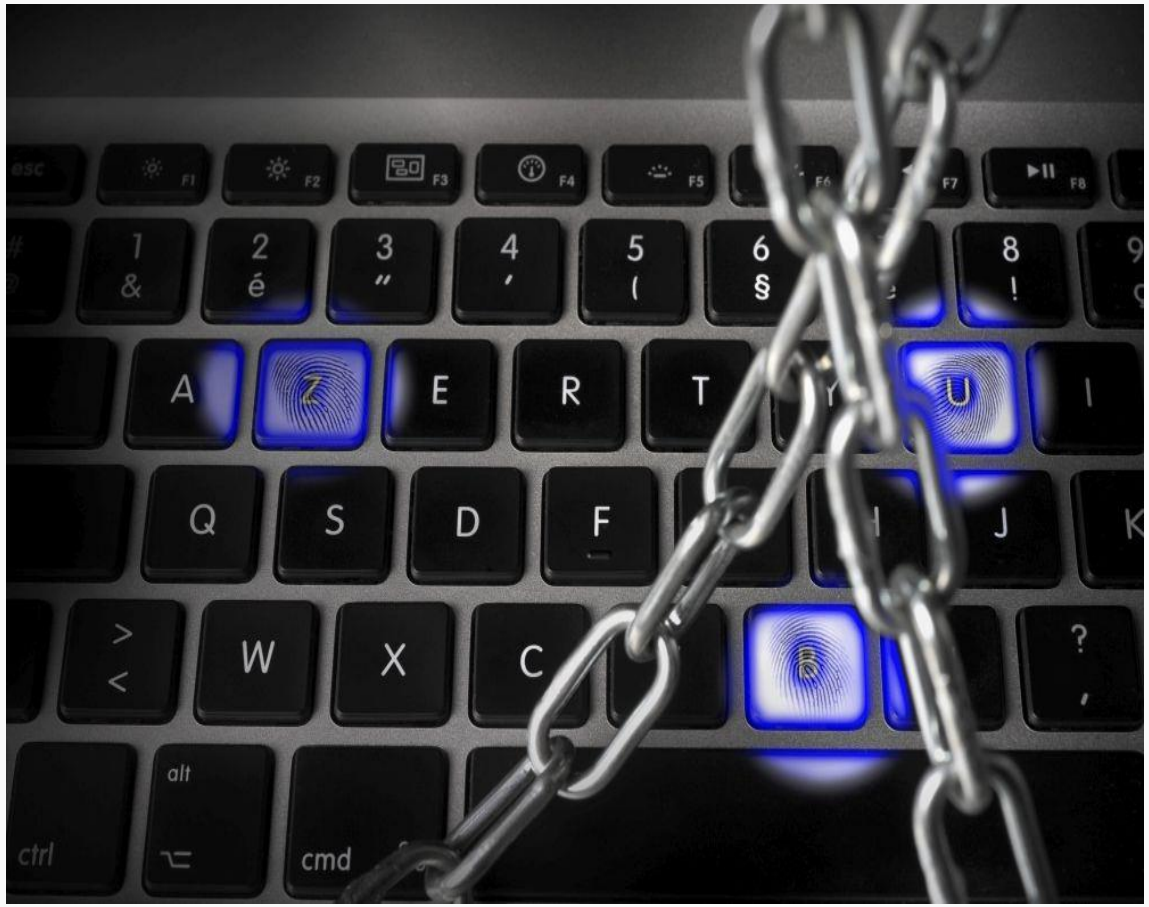
FASI DI GESTIONE DI UN ATTACCO

- 0) Stipulare un contratto o prendere accordi per fare la telefonata a tempo zero
- 1) Isolamento e contenimento
- 2) Valutazione dell'impatto
- 3) Notifiche alle autorità competenti
- 4) Ripristino di dati e sistemi
- 5) Analisi forense e miglioramenti (continui) sulla sicurezza
- 6) Lezione appresa e (eventuale) condivisione

- 7) Prepararsi all'eventuale ispezione del Garante

COSTI DI UN ATTACCO

1) Eventuale riscatto
2) Spese per il Response Team, le attività sistemistiche di ripristino infrastruttura, i tecnici per le postazioni di lavoro
3) Perdite legate all'interruzione dell'attività
4) Costi per analisi forense e per gestione Privacy
5) Costi per maggior utilizzo del personale interno (straordinari): nel nostro caso 840 ore di cui 150 della E.Q., le mie non le ho neppure contate
6) Danni reputazionali
7) Investimenti e spese per incremento della sicurezza
8) Franchigie e premi per assicurazione Cyber



SI POTREBBERO DIRE TANTE COSE, ne citiamo alcune

- Sarebbe meglio non farsi attaccare (prevenzione), ma la sicurezza al 100% non esiste
- Porre una particolare attenzione ai backup (non è facile ora che le cose non sono più in casa)
- Il punto debole è quasi sempre l'utente generico
- Occorre fare formazione mirata (utenti generici, dirigenti e E.Q., politici, personale IT)
- Sviluppare una cultura diffusa sulla privacy e sulla sicurezza, le due cose vanno a braccetto
- Coltivare le competenze del personale IT
- La sicurezza costa, e tanto, ma un incidente può costare molto di più o addirittura non avere prezzo
- Fidatevi di ACN e Polizia Postale

GRAZIE