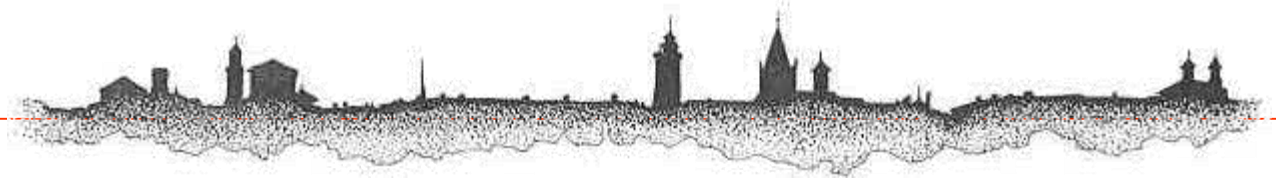
Città di Cuneo

GDPR : principali minacce e misure tecniche

Il nuovo Regolamento europeo sulla tutela dei dati personali e le misure minime di sicurezza da adottare nell'ambiente di lavoro



Città di Cuneo

Sicurezza informatica nella PA e riferimenti normativi

D. Lgs. **196/2003** ***Codice in materia di protezione dei dati personali***

D. Lgs. **259/2003** ***Codice delle Comunicazioni elettroniche***

D. Lgs. **82/2005** ***Codice dell'amministrazione digitale*** successivamente integrato e modificato dai D. Lgs. 179/2016 e 217/2017

DPCM 24 gennaio **2013** ***Quadro strategico nazionale per la sicurezza dello spazio cibernetico*** e ***Piano nazionale per la protezione cibernetica e la sicurezza informatica***

Direttiva 1 agosto **2015** del Presidente del Consiglio dei Ministri ***Attuazione degli indirizzi strategici ed operativi del DPCM 24 gennaio 2013***

GU Serie Generale n.103 del 05-05-**2017** ***Misure minime di sicurezza ICT per le pubbliche amministrazioni*** redatte da AgID

D. Lgs. **51/2018** ***Attuazione della direttiva (UE) 2016/680 Regolamento generale sulla protezione dei dati***

D. Lgs. **65/2018** ***Attuazione della direttiva (UE) 2016/1148 Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*** (Direttiva NIS)

D. Lgs. **101/2018** ***Disposizioni per l'adeguamento della normativa nazionale (196/2003) alle disposizioni del regolamento (UE) 2016/679***

2002

Direttiva 2002/58/CE Trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche

2004

Regolamento 2004/460 European Network and Information Security Agency (ENISA)

2013

Piano di sicurezza informatica dell'UE per garantire un elevato livello di *network and information security* (NIS)

2015

Accordo sulla prima normativa UE relativa alla cybersecurity (NIS)

2016

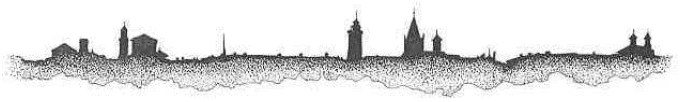
Regolamento 2016/679 (GDPR) **Direttiva 2016/1148** (NIS)

2017

Adozione di un cybersecurity package per garantire resilienza, deterrenza e difesa **Proposta di creazione di un cybersecurity certification framework**

2018

Approvazione entro fine anno di un «Regolamento sulla cybersecurity» per istituire una certificazione ICT a livello UE



Città di Cuneo

CERT Nazionale, CERT-PA e CSIRT

CERT nazionale Italia

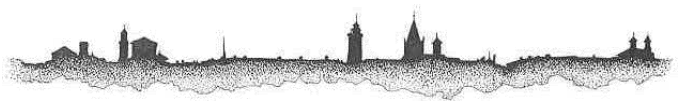
- *Individuato presso il **Ministero dello sviluppo economico** ai sensi dell'art. 16 bis del d.lgs. 259/2003 (Codice delle Comunicazioni elettroniche)*
- ***Attivo dal 5 giugno 2014** presso l'Istituto Superiore delle comunicazioni e delle tecnologie, opera **a supporto di Cittadini ed Imprese***
- *Fornisce **informazioni su potenziali minacce informatiche**, **raccomandazioni**, **consigli** e **contromisure** per la prevenzione e la risoluzione di incidenti informatici*
- *Opera sulla base di un **modello cooperativo pubblico-privato** e collabora con CERT-PA, CSIRT, CERT Difesa, CNAIPIC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche), CERT EU, CERT extra UE e importanti imprese che gestiscono infrastrutture informatizzate*

COMPUTER EMERGENCY RESPONSE TEAM
PUBBLICA AMMINISTRAZIONE
CERT - PA

- *Opera all'interno di **AgID** in linea con il modello organizzativo previsto dal DPCM 24 gennaio 2013 (Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale)*
- ***Attivo dal 3 marzo 2014**, opera **a supporto delle Pubbliche Amministrazioni***
- ***Attivo dal 3 marzo 2014**, fornisce alle PA richiedenti supporto per la **definizione dei processi di gestione della sicurezza**, **bollettini** e **segnalazioni di sicurezza**, **gestione di allarmi di sicurezza** e **formazione***

CSIRT Italia

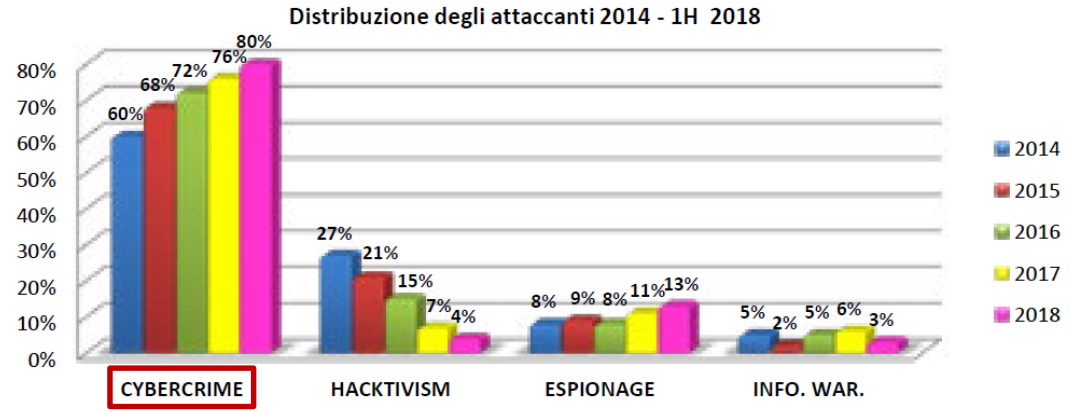
- *Sarà istituito presso la **Presidenza del Consiglio dei Ministri** ai sensi del d.lgs 65/2018 (Attuazione Direttiva UE NIS 2016/1148) mediante unificazione del CERT Nazionale e del CERT-PA*
- *Entro il **9 novembre 2018** sarà adottato un DPCM che definirà la sua organizzazione*
- ***CERT Nazionale** e **CERT-PA** nella fase transitoria **continuano a svolgere compiti di prevenzione e risposta ad incidenti informatici** e congiuntamente **gestiscono le notifiche di incidenti informatici**, che nella fase transitoria hanno carattere obbligatorio solo per i fornitori di servizi digitali*

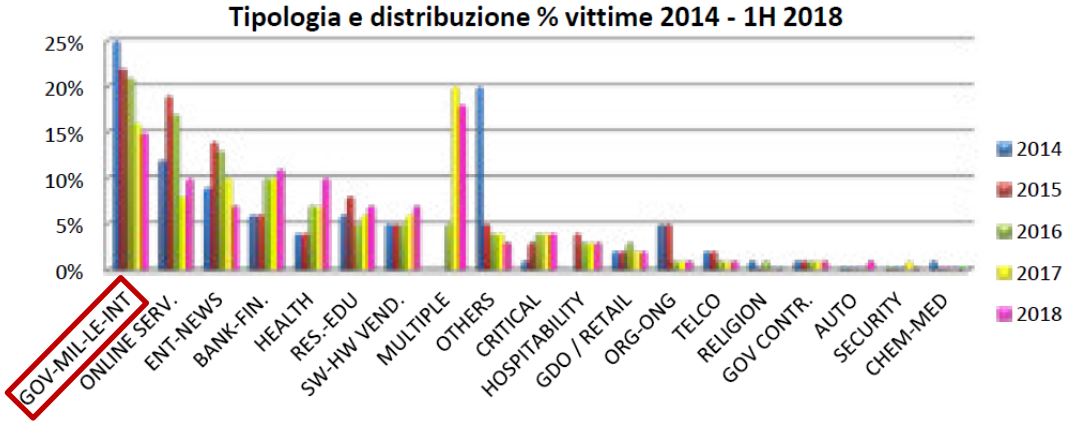


Città di Cuneo

Rapporto Clusit Settembre 2018

Analisi basata su oltre 7.595 attacchi di dominio pubblico classificati come gravi dal Clusit tra gennaio 2011 e giugno 2018 di cui oltre 1.127 solo nel 2017 (+7,33% rispetto al 2016) e 730 nel primo semestre 2018





Confronto 1° semestre 2018 – 2° semestre 2017

Attacchi (2H 2017: 554 – 1H 2018: 730)	+31,77%
Espionage/Sabotage	+69,09%
Cybercrime	+35,25%
Automotive	+200,00%
Research - Education	+128,57%
Hospitability	+69,23%
Health	+62,22%
Gov - Mil - LEAs - Intelligence	+52,05%
0-day	+140,00%
Unknown	+54,74%
Multiple Techniques / APT	+48,15%
Vulnerabilities / Misconfigurations	+37,50%
Malware	+22,78%
Phishing / Social Engineering	+22,00%

Severity attacchi nel 1° semestre 2018 e confronto con 2017

Medium 57% (+9%) **High 22% (-9%)** **Critical 21% (+0%)**

Impatto geopolitico, sociale, economico, di immagine e di costo/opportunità per le vittime

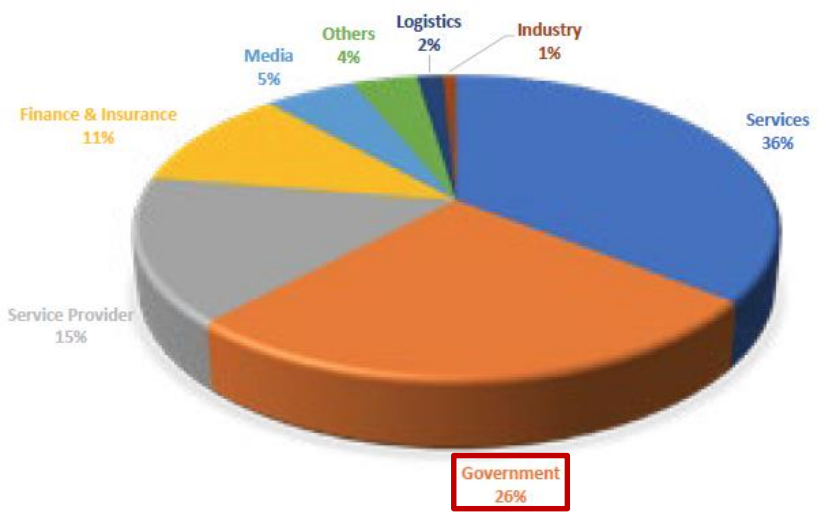
Città di Cuneo

Analisi Fastweb 2017 e principali DataData breaches 2018

Analisi basata su oltre 35 milioni di eventi di sicurezza (+50% rispetto 2016) da cui emergono:

- **Trend di crescita degli attacchi importanti (+11% rispetto a 2016)**
- **Tra i principali attacchi si confermano quelli di tipo «ransomware» (riscatto per accedere ai dati)**
- **Trend di crescita dei malware così detti «miners» (sfruttamento della capacità di elaborazione)**

Target di possibili attacchi DDoS del 2017



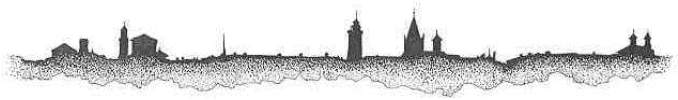
Il 95% degli attacchi è durato meno di 3 ore, il 3% oltre le 24 ore

IP classificati come fonte di e-mail SPAM

40.000 IP sono stati inseriti almeno una volta in blacklist nel 2017

2017 2018 **Data breaches**

DEC	GEN	FEB	MAR	APR	MAG	GIU	LUG	AGO	SET	OTT	NOV
Breach Compilation	MailChimp	FedEx Boeing Western Union	Facebook Miur	Twitter	Philips	Ticketfly	American Express Salesforce	Instagram Apple	Facebook United Nations Veeam	Facebook Google Plus	PA italiane Siae PEC



Città di Cuneo

Esempi di attacchi ad enti locali italiani nel 2018

GEN
Sa 13

Attacco al sito del Comune di Vallo della Lucania

Danno: *Blocco del sito istituzionale da parte del gruppo Persian Hackers*

Conseguenze: *Sito non disponibile per alcune ore*

Pop: 9.000

FEB
Me 21

Ransomware al Comune di Termini Imerese

Danno: *Danneggiato in modo irreparabile il sistema che gestisce degli uffici ragioneria, tributi e personale*

Conseguenze: *Stipendi erogati con alcuni giorni di ritardo, perdita dei dati del bilancio consuntivo 2016 con conseguente ritardo nell'approvazione del documento contabile*

Pop: 26.000

MAR
Me 14

Attacco al sito del Comune di Portici

Danno: *Pubblicazione sul sito istituzionale del manifesto di AnonPlus, alterazione ripetuta di contenuti*

Conseguenze: *Sito offline per alcune ore*

Pop: 55.000

APR
Sa 21

Ransomware al Comune di Massa Lubrense

Danno: *Criptati i file di Office e Pdf sul server e le copie di backup*

Conseguenze: *Albo pretorio bloccato per diversi giorni, pubblicazione temporanea dei provvedimenti nella sezione Avvisi, Bandi e Concorsi del sito istituzionale*

Pop: 14.000

APR
Me 25

Attacco al sito del Comune di Bologna

Danno: *Pubblicazione sul sito istituzionale del manifesto di AnonPlus, alterazione ripetuta di contenuti*

Conseguenze: *Sito offline per alcuni giorni, proroga del termine per la presentazione delle domande d'iscrizione e trasferimento ai nidi d'infanzia comunali*

Pop: 390.000

GIU
Gi 7

Attacco al sito del Comune di Cassola

Danno: *Pubblicazione sul sito istituzionale del manifesto di AnonPlus*

Conseguenze: *Sito offline per alcune ore*

Pop: 15.000

LUG
Ma 10

Virus su server del Comune di Lacco Ameno

Danno: *Server comunale non funzionante per giorni*

Conseguenze: *Impossibile l'utilizzo dei computer, rubate le copie delle multe dal sistema della Polizia Municipale, un hacker ha cercato di allearsi con gli automobilisti ischitani sanzionati cancellando le multe*

Pop: 5.000

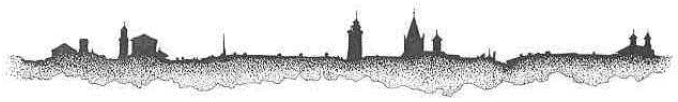
SET
Sa 8

Attacco al sito del Comune di Sant'Agnello

Danno: *Frase volgare nella sezione 'Notizie in tempo reale'*

Conseguenze: *Il messaggio volgare è rimasto online per diverse ore ed è stato rimosso solamente dopo segnalazioni e lamentele da parte della cittadinanza sui social*

Pop: 9.000



Città di Cuneo

Metodologie di attacco e di difesa

Dove

- Mail
- Siti
- Chiavette USB

Quando

- Inizio settimana
- Fine settimana
- Prima festività
- Dopo festività

Come

- Link
- File Office
- File Zip
- File PDF
- Autoplay

Diffidare

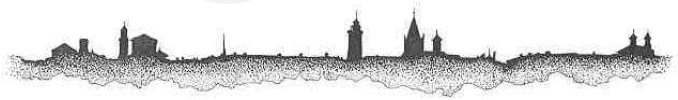
- Mail da sconosciuti
- Mail inattese o non pertinenti
- Chiavette USB estranee all'ufficio

Verificare

- Pertinenza mail
- Attendibilità mail tramite chiamata telefonica
- Esistenza file sospetti su PC o rete

Evitare

- Apertura link, file sospetti senza verifica antimalware (VirusTotal)
- Rispondere a mail sospette



Città di Cuneo

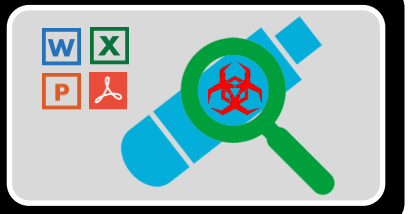
Esempi di casi reali

Business E-mail / PEC Compromesse
Richieste da aziende professionisti conosciuti inviate a loro insaputa con documenti contraffatti (ordini, fatture, etc.), richiedono variazioni di pagamenti, inoltrano file/link malevoli

E-mail in apparenza da studi legali / Procura della Repubblica
Inducono a scaricare file contenenti documenti legali per veicolare malware sul computer della vittima

E-Mail estorsive
Richieste di pagamenti per evitare diffusione di materiale riservato o compromettente, talvolta come prova viene indicata una password utilizzata in passato

Collegamenti a file malevoli su chiavette USB
Collegamenti a malware mascherati con icone di file Office o PDF per infettare il computer della vittima



Città di Cuneo

Gestione delle credenziali

Modificare password

- **Compromissione** di servizi utilizzati a livello istituzionale o personale
- **Anomalie**
  - Accessi inaspettati
  - Blocchi account inspiegabili
  - Possibile conoscenza della password da parte di terzi
- Credenziali istituzionali o personali presenti in **data breach**

haveibeenpwned.com
hacked-emails.com

Come impostare le password

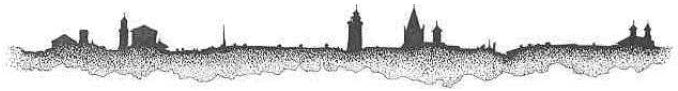
- Rispettare la **complessità**
- **Diversificare** le password
- **Evitare** password riconducibili all'**utente**
- **Evitare** password riconducibili al **servizio**
- **Evitare** password di **uso comune**
- **Evitare** password generate con una **regola intuibile**
- Generare la password ipotizzando che le **precedenti siano note**
- Quando possibile usare **password randomiche**
- **Modificare** password generate da tool

www.passwordrandom.com

Random Meter Top

Conformità delle password al GDPR

In base all'Art. 32 la password è una misura tecnica e quindi essere «adeguata al fine di garantire un livello di sicurezza adeguato al rischio di accesso non autorizzato»



Città di Cuneo

Misure minime di sicurezza ICT per le pubbliche amministrazioni

Roma - Venerdì, 5 maggio 2017 Anno 158° - Numero 103
GAZZETTA UFFICIALE
DELLA REPUBBLICA ITALIANA

ABSC 1 (CSC 1)
Inventario dei dispositivi autorizzati e non autorizzati

ABSC 2 (CSC 2)
Inventario dei software autorizzati e non autorizzati

ABSC 3 (CSC 3)
Proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server

ABSC 4 (CSC 4)
Valutazione e correzione continua della vulnerabilità

ABSC 5 (CSC 5)
Uso appropriato dei privilegi di amministratore

ABSC 8 (CSC 8)
Difese contro i malware

ABSC 10 (CSC 10)
Copie di sicurezza

ABSC 13 (CSC 13)
Protezione dei dati

Esempi di misure minime

ABSC 2

"Whitelist" applicazioni autorizzate *e rilevazione software non autorizzato*

ABSC 3

Configurazioni sicure standard *per la protezione dei sistemi operativi*

ABSC 4

Ricerca e risoluzione vulnerabilità, installazione aggiornamenti *per il sistema operativo e applicazioni*

ABSC 5

Limitare i privilegi di amministrazione *agli utenti con competenze e necessità operativa di configurazione****, tutte le utenze, devono essere nominative*** *e riconducibili ad una sola persona*

ABSC 8

Bloccare i tipi di file potenzialmente pericolosi *e non strettamente necessari nella posta elettronica e nel traffico web,* ***disattivare l'esecuzione automatica dei contenuti dinamici*** *nei file(macro),* ***disattivare l'apertura automatica delle mail****,* ***disattivare l'anteprima automatica dei contenuti dei file***

ABSC: Agid Basic Security Control **CSC**: Critical Security Control (SANS Institute)

Città di Cuneo

Privacy e cybersecurity nella Pubblica Amministrazione

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

*"La **vulnerabilità dimostrata da diverse amministrazioni pubbliche** in questi giorni è frutto di molti fattori ma, soprattutto, delle modalità con le quali il processo di digitalizzazione si è sviluppato nel nostro Paese, in **assenza di un piano organico e di investimenti adeguati**, **tanto sotto il profilo tecnologico quanto riguardo al fattore umano**. Per rafforzare i confini digitali del Paese è necessaria una **strategia di lungo periodo che vada oltre la mera infrastrutturazione e razionalizzi il patrimonio informativo pubblico**, in particolare **secondo principi di privacy by design**, per ridurre la superficie di attacco, assumendo la resilienza informatica e la protezione dei dati, quali obiettivi centrali dell'azione di Governo. **La negligenza rispetto alla sicurezza informatica e cibernetica non è più tollerabile** in un contesto in cui le relazioni ostili tra Paesi si giocano in primo luogo sul piano digitale e in cui, anche per questo, la disciplina di protezione dati (oltre a quella sulla cybersecurity) assumono come modello d'intervento l'**approccio basato sulla prevenzione del rischio**. Non si tratta, evidentemente, di meri adempimenti formali, ma di **misure essenziali per rendere il Paese competitivo e proteggere, unitamente alla persona, la sicurezza nazionale**."*

Antonello Soro, Presidente Autorità Garante per la protezione dei dati personali
«Nuovo attacco di Anonymous Italia: diffusi i dati di ministeri e polizia - La Repubblica 6 novembre 2018»