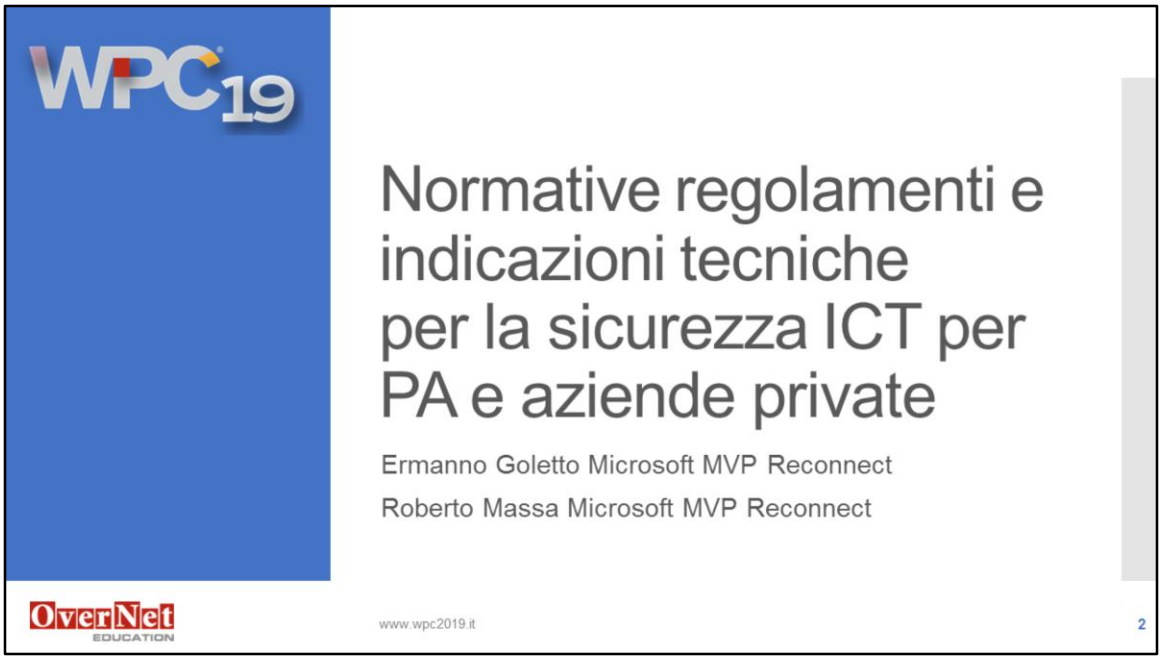
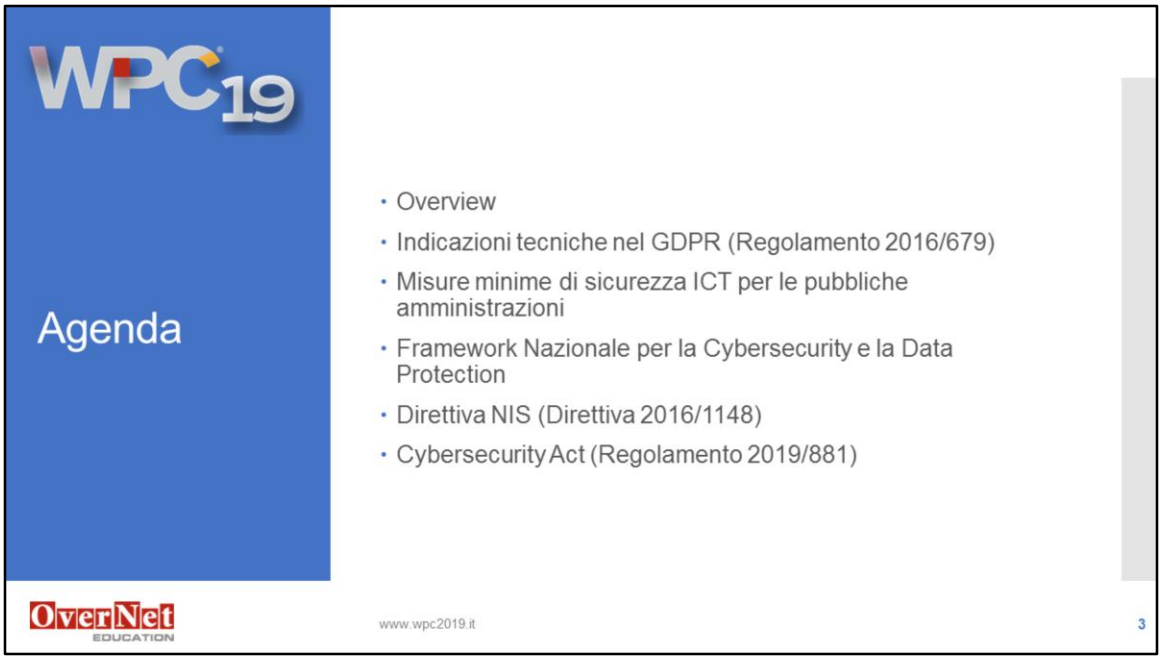
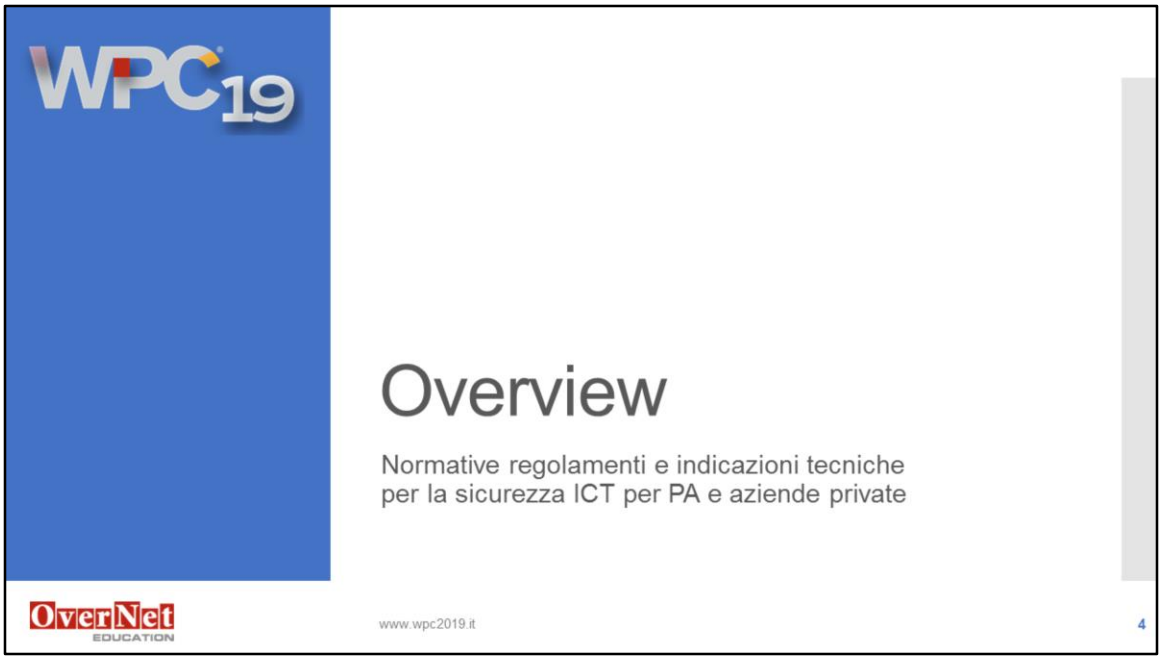

WPC19
Milano
3.4.5.Dicembre


WPC19
Normative regolamenti e indicazioni tecniche per la sicurezza ICT per PA e aziende private
Ermanno Goletto Microsoft MVP Reconnect
Roberto Massa Microsoft MVP Reconnect
OverNet EDUCATION
www.wpc2019.it
2


WPC19
Agenda
• Overview
• Indicazioni tecniche nel GDPR (Regolamento 2016/679)
• Misure minime di sicurezza ICT per le pubbliche amministrazioni
• Framework Nazionale per la Cybersecurity e la Data Protection
• Direttiva NIS (Direttiva 2016/1148)
• Cybersecurity Act (Regolamento 2019/881)
OverNet EDUCATION
www.wpc2019.it
3


WPC19
Overview
Normative regolamenti e indicazioni tecniche
per la sicurezza ICT per PA e aziende private
OverNet
EDUCATION
www.wpc2019.it
4

Cybersecurity e riferimenti normativi

CERT Nazionale, CERT-PA e CSIRT

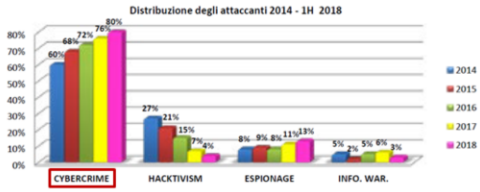
- *Individuato presso il **Ministero dello sviluppo economico** ai sensi dell'art. 16 bis del d.lgs. 259/2003 (Codice delle Comunicazioni elettroniche)*
- ***Attivo dal 5 giugno 2014** presso l'Istituto Superiore delle comunicazioni e delle tecnologie, opera **a supporto di Cittadini ed Imprese***
- *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*

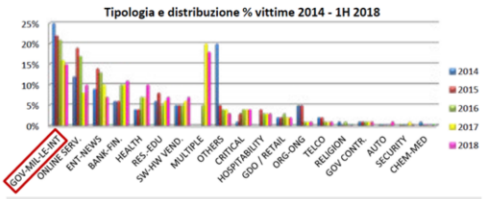
- *Opera all'interno di **AgID** in linea con il modello organizzativo previsto dal DPCM 24 gennaio 2013 (Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale)*
- ***Attivo dal 3 marzo 2014**, opera **a supporto delle Pubbliche Amministrazioni***
- ***Attivo 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***

- *Costituito 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** sarà adottato un provvedimento definirà la sua organizzazione*
- ***CERT Nazionale** e **CERT-PA** nella frattempo assolvono congiuntamente il ruolo e le funzioni del CSIRT Italiano, ovvero **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*

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





Severity attacchi nel 1° semestre 2018 e confronto con 2017

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

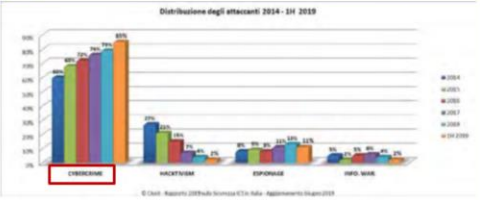
Impatto geopolitico, sociale, economico, di immagine e di costo/opportunità per le vittime

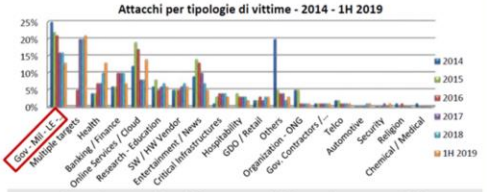
Confronto 1° semestre 2018 – 2° semestre 2017

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%

Rapporto Clusit Settembre 2019

Analisi basata su oltre 9.174 attacchi di dominio pubblico classificati come gravi dal Clusit tra gennaio 2011 e giugno 2019 di cui oltre 1.552 solo nel 2018 (+37,7% rispetto al 2017) e 757 nel primo semestre 2019





Severity attacchi nel 1° semestre 2019 e confronto con 2018

Medium 46% (+7%) **High 28% (-5%)** **Critical 26% (-2%)**

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

Confronto 1° semestre 2019 – 1° semestre 2018

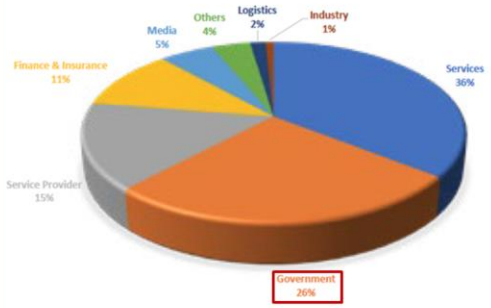
Attacchi (1H 2018: 747 – 1H 2019: 757)	+1,3%
Cybercrime	+8,3%
Others	+73,3%
Online Services / Cloud	+49,3%
Healthcare	+31,1%
Multiple targets	+16,3%
Phishing / Social Engineering	+104,8%
Account Hacking / Cracking	+88,9%

Analisi Fastweb 2017

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

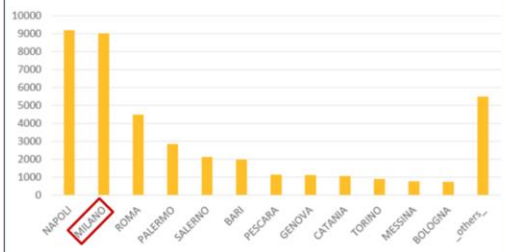
- Trend di crescita degli attacchi importanti (+11% rispetto a 2016)
- Tra i principali attacchi si confermano quelli di tipo «ransomware» (riscatto per accedere ai dati)
- Trend di crescita dei malware così detti «miners» (sfruttamento della capacità di elaborazione)

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



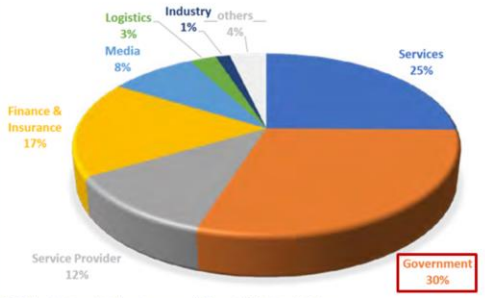
40.000 IP sono stati inseriti almeno una volta in blacklist nel 2017

Analisi Fastweb 2018

Analisi basata su oltre 40 milioni di eventi di sicurezza (+14% rispetto al 2017) da cui emergono:

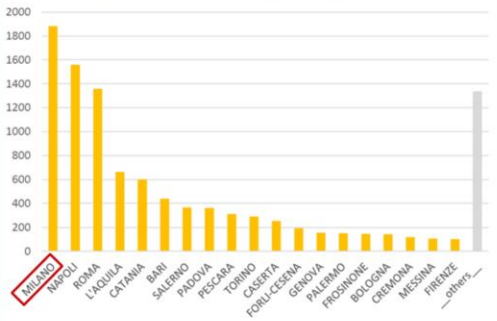
- Evoluzione dei Malware e Botnet con diffusione massiva di nuovi malware, sono state individuate 212 famiglie di malware (+10% rispetto al 2017)
- Tra i principali attacchi si confermano quelli di tipo «ransomware» (Wannacry seguito da Gozi e Ramnit) e «miners» (infezioni di tipo crypto-jacking)
- Trend di crescita degli attacchi di tipo «APT» (Advanced Persistent Threat) mirati a soggetti specifici che utilizzano tecniche di spear phishing
- 19% di software malevoli non ancora catalogati e di cui non si conoscono tutti i dettagli (+11% rispetto al 2017)

Target di possibili attacchi DDoS del 2018

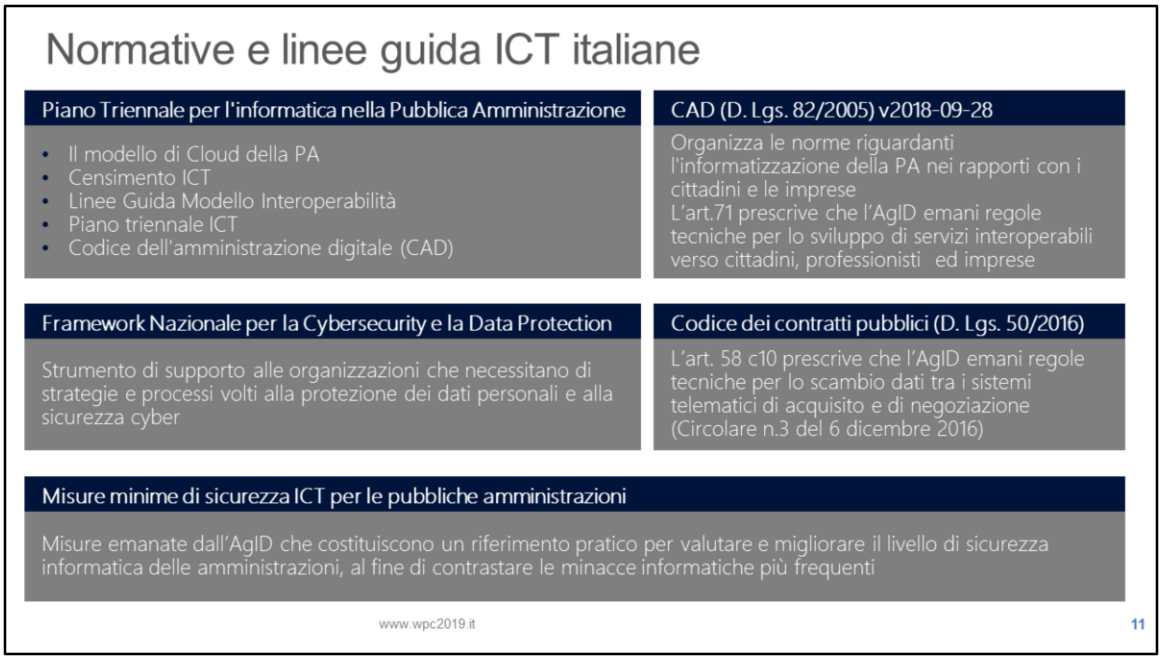


Il 95% degli attacchi è durato meno di 3 ore, il 2% oltre le 24 ore (+3% rispetto al 2017 degli attacchi di breve durata)

IP classificati come fonte di e-mail SPAM



10.500 IP sono stati inseriti almeno una volta in blacklist nel 2018 (-73,75% rispetto al 2017)



https://www.agid.gov.it/sites/default/files/repository_files/regole_tecniche/regole_tecniche_colloquio_e_scambio_dati_piattaforme_e-procurement.pdf

il modello Cloud della PA,

- modello strategico che si compone di infrastrutture e servizi qualificati da AgID sulla base di un insieme di requisiti volti a garantire elevati standard di qualità per la PA;

Censimento del patrimonio ICT

- Circolare n.1 del 14 giugno 2019 - Censimento del patrimonio ICT delle Pubbliche Amministrazioni e classificazione delle infrastrutture idonee all'uso da parte dei Poli Strategici Nazionali
- Datacenter classificati in Gruppo A e Gruppo B **con carenze strutturali e/o organizzative**

Linee Guida Modello Interoperabilità

- Si riferiscono allo European Interoperability Framework (EIF) fornisce orientamenti alle PA Europee su come operare le iniziative relative al tema dell'interoperabilità;

L'ambito di applicazione dell'EIF comprende tre tipi di interazioni:

- **A2A (*amministrazione-amministrazione*), ossia le interazioni tra PA;**
- **A2B (*amministrazione-impresa*), ossia le interazioni tra le PA e le imprese;**
- **A2C (*amministrazione-cittadino*), ossia le comunicazioni tra le PA e i cittadini.**

Il Piano Triennale ICT 2019-2021

- novità il recepimento delle ultime modifiche introdotte del Codice dell'Amministrazione Digitale (CAD) e delle recenti direttive e regolamenti europei sull'innovazione digitale;
- il rafforzamento del paradigma Cloud della PA con l'applicazione del principio *cloud first*;
- la definizione di Modelli e strumenti per l'innovazione per la PA con un'attenzione ai temi dell'*open innovation, dell'innovation procurement* e al paradigma *smart landscape*;

Framework Nazionale per la Cybersecurity e la Data Protection
ispirato al Cybersecurity Framework ideato dal NIST


WPC19
Indicazioni tecniche nel GDPR
Normative regolamenti e indicazioni tecniche per la sicurezza ICT per PA e aziende private
OverNet EDUCATION
www.wpc2019.it
12

Articolo 17 Paragrafo 1 e 2

Diritto alla cancellazione («diritto all'oblio») (C65, C66)

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
   a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
   b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
   c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
   d) i dati personali sono stati trattati illecitamente;
   e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
   f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.
2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

Eliminazione dati

Backup e diritto all'oblio

- L'**autorità danese Data Inspectorate** afferma che **la cancellazione dei dati dei record dai backup è obbligatoria "se ciò è tecnicamente possibile"**
- Secondo l'**autorità francese CNIL** (Commission Nationale Informatique et Libertés) **le organizzazioni non devono necessariamente eliminare i backup a fronte di una richiesta di cancellazione**. Tuttavia, **le organizzazioni dovranno spiegare chiaramente all'interessato** (usando un linguaggio semplice e chiaro) **che i suoi dati personali sono stati rimossi dai sistemi di produzione, ma una copia di backup potrebbe rimanere**, e scadrà dopo un certo periodo di tempo (il tempo di conservazione va indicato nella comunicazione con l'interessato)
- Altre autorità di controllo potrebbero avere una posizione in merito differente e più rigida
- **Per essere in grado di dimostrare che non è pratico eliminare i dati di backup bisogne condurre una valutazione del rischio e una valutazione d'impatto sul business**
- **Occorre documentare le politiche e le procedure per mantenere sicuri i dati di backup, con apposite istruzioni sulla crittografia dei backup e sul luogo di mantenimento dei dispositivi di backup**

https://www.garanteprivacy.it/temi/diritto-all-oblio

https://blog.quantum.com/backup-administrators-the-1-advice-to-deal-with-gdpr-and-the-right-of-erasure

https://www.cybersecurity360.it/legal/privacy-dati-personali/backup-e-diritto-alloblio-alla-luce-del-gdpr/

Articolo 19

Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento (C31)

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Notifica

Articolo 20

Diritto alla portabilità dei dati (C68)

1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:
   a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e
   b) il trattamento sia effettuato con mezzi automatizzati.
2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.
3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

Formato dati di uso comune

Trasmissione diretta dei dati

Articolo 21

Diritto di opposizione (C69, C70)

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.
3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.
4. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.
5. Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.
6. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Blocco del trattamento dei dati

Articolo 22

Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione (C71, C72)

1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
2. Il paragrafo 1 non si applica nel caso in cui la decisione:
   a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
   b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
   c) si basi sul consenso esplicito dell'interessato.
3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.
4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

Bypass decisioni automatizzate

Articolo 25

Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita (C75-C78)

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

Pseudonimizzazione	Trattamento dei soli dati necessari	Accessibilità limitata

Articolo 32 Paragrafo 1

Sicurezza del trattamento (C83)

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Pseudonimizzazione e Cifratura | Riservatezza, Integrità, Disponibilità e Resilienza | Ripristino

Articolo 32 Paragrafi 2,3,4

Sicurezza del trattamento (C83)

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.
4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Valutazione livello sicurezza | Istruzione

Articolo 33 Paragrafi 1, 2

Notifica di una violazione dei dati personali all'autorità di controllo (C85, C87, C88)

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Monitoraggio | Rilevamento, Correlazione e Analisi

Articolo 33 Paragrafi 3, 4, 5

Notifica di una violazione dei dati personali all'autorità di controllo (C85, C87, C88)

3. La notifica di cui al paragrafo 1 deve almeno:
   a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
   b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
   c) descrivere le probabili conseguenze della violazione dei dati personali;
   d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Incident Report	Post-Incident Activity

Articolo 34

Comunicazione di una violazione dei dati personali all'interessato (C86-C88)

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
   a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
   b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
   c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Cifratura | Contenimento, Sradicamento e Ripristino


WPC19
Misure minime di sicurezza ICT per le pubbliche amministrazioni
Normative regolamenti e indicazioni tecniche per la sicurezza ICT per PA e aziende private
OverNet EDUCATION
www.wpc2019.it
25

Overview

Già anticipate via Web sin da settembre 2016

Emesse con circolare 18 aprile 2017, n. 2/2017

Gazzetta Ufficiale (SG) n.103 del 5/5/2017

Adozione obbligatoria per tutte le PP. AA.

Adeguamenti entro il 31/12/2017

- Basate sull'insieme di controlli SANS 20, pubblicato dal Center for Internet Security come CCSC «CIS Critical Security Controls for Effective Cyber Defense» versione 6.0 ottobre 2015
- Il SANS20 è un elenco composto da venti controlli, denominati Critical Security Control (CSC), ordinato sulla base dell'impatto sulla sicurezza dei sistemi
- Ciascun controllo precede tutti quelli la cui implementazione innalza il livello di sicurezza in misura inferiore alla sua
- Nell'identificazione degli ABSC ci si è riferiti alla versione 6 dei CCSC. Tuttavia l'insieme dei controlli definiti è più vicino a quello della versione 5.1 poiché AgID ha ritenuto che molti dei controlli eliminati nel passaggio alla nuova versione anche se non più attuali nella realtà statunitense, sono ancora importanti nel contesto della pubblica amministrazione italiana

- Primo progetto 2008 Inizialmente curato da **SANS**
- Trasferita la competenza al Council on Cyber Security (CCS) in 2013
- E successivamente trasferita ancora al Center for Internet Security (CIS) in 2015

The **SANS Institute** (officially the **Escal Institute of Advanced Technologies**)
Organizzazione a fini di Lucro
in Italia I controlli sono declinati con **ABSC Agid Base Security Controls**

Strutturazione delle Misure minime di sicurezza ICT

- Il CCSC è stato concepito essenzialmente nell'ottica di prevenire e contrastare gli attacchi cibernetici, non viene data particolare rilevanza agli eventi di sicurezza dovuti a casualità quali guasti ed eventi naturali
- Ai controlli delle prime cinque classi AgID ha deciso di aggiungere quelli relativi alle difese contro i malware (CSC8), quelli delle alle copie di sicurezza (CSC10) e quelli riferiti alla protezione dei dati rilevanti contro i rischi di esfiltrazione (CSC13)
- Ciascun CSC è costituito da una famiglia di misure di dettaglio più fine che possono essere adottate in modo indipendente, AgID ha ritenuto che anche al secondo livello ci fosse una granularità ancora eccessiva, che avrebbe costretto le piccole amministrazioni ad introdurre misure esagerate per la propria organizzazione
- E' stato introdotto un ulteriore terzo livello nel quale la misura di secondo livello viene decomposta in misure elementari implementabili in modo indipendente
- Un ABSC è identificato da un identificatore gerarchico a tre livelli x, y, z
  - x e y sono i numeri che identificano il CSC corrispondente
  - z individua ciascuno dei controlli di livello 3
- Le Misure minime di sicurezza ICT sono composte da 8 ABSC che sono derivati dai CSC 1,2,3,4,5,8,10 e 13
- Viene indicato quali controlli implementare per ottenere un determinato livello di sicurezza:
  - «Minimo» specifica il livello sotto il quale nessuna amministrazione può scendere, i controlli in essa indicati debbono riguardarsi come obbligatori
  - «Standard» può essere assunta come base di riferimento nella maggior parte dei casi
  - «Alto» può essere considerata come un obiettivo a cui tendere
- Le amministrazioni NSC (Nucleo di Sicurezza Cibernetica), per l'infrastruttura che gestisce dati NSC, dovrebbero collocarsi almeno a livello "standard" in assenza di requisiti più elevati

27

Formato delle Misure minime di sicurezza ICT

ABSC 10 (CSC 10): COPIE DI SICUREZZA

Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.

3 livelli

ABSC_ID		#	Descrizione	FNSC	Min.	Std.	Alto
10	1	1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	PR.IP-4	X	X	X
		2	Per assicurare la capacità di ripristino di sistemi IT critici devono riguardare il sistem	PR.IP-4			X
		3	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	PR.IP-4			X
	2	1	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	PR.IP-4		X	X
	3	1	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud. .	PR.DS-6	X	X	X
	4	1	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	PR.AC-2 PR.IP-4 PR.IP-5 PR.IP-9	X	X	X

Subcategory del Framework Core del Framework nazionale per la Cyber Security

Livello di sicurezza

28

ABSC 1 (CSC 1)

Inventario dei dispositivi autorizzati e non autorizzati

1.1.1 Inventario delle risorse attive | 1.1.2 Inventario automatizzato | 1.1.3 Discovery dispositivi in rete con allarmi su anomalie

1.1.4 Qualificazione sistemi in rete tramite analisi del traffico

1.2.1 Logging DHCP | 1.2.2 Utilizzo Logging DHCP per migliorare inventario

1.3.1 Aggiornare l'inventario quando sono connessi nuovi dispositivi approvati

1.3.2 Inventario automatizzato automaticamente quando sono connessi nuovi dispositivi approvati

1.4.1 Registrare indirizzo IP di tutti i sistemi e dispositivi in rete

1.4.2 Registrare hostname, funzione, responsabile, ufficio, tipologia (portatile/personale) dei dispositivi con indirizzo IP

1.4.3 Identificare telefoni cellulari, tablet, laptop e altri dispositivi portatili che memorizzano o elaborano dati

1.5.1 Autenticazione a livello di rete 802.1x correlata all'inventario per distinguere i sistemi autorizzati

1.6.1 Certificati lato client per validare e autenticare i sistemi prima della connessione alla rete locale

ABSC 2 (CSC 2):

Inventario dei software autorizzati e non autorizzati

2.1.1 Elenco software autorizzati con versione per tipo di sistema, non consentire installazione software non in elenco

2.2.1 "Whitelist" (anche ampia) applicazioni autorizzate, bloccare esecuzione software non lista

2.2.2 "Whitelist" mirata per sistemi con funzioni specifiche

2.2.3 Verifica integrità file applicazioni in "whitelist" per verificare che non siano state modificate

2.3.1 Scansioni regolari per rilevare presenza software non autorizzato

2.3.2 Inventario software completo

2.3.3 Inventario software automatizzato che registri versione OS, applicazioni installate e livello patch

2.4.1 VM e/o sistemi air-gapped (isolati) per eseguire applicazioni dedicate a operazioni strategiche o critiche

ABSC 3 (CSC 3)

Proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server

3.1.1 Utilizzo di configurazioni sicure standard

3.1.2 Configurazioni sicure standard "hardened" OS/applicazioni (eliminazione account utente/servizio non necessari, disattivazione/eliminazione servizi non necessari, configurazione stack/heaps non eseguibili, applicazione patch, chiusura porte di rete non utilizzate

3.1.3 Validazione/aggiornamento regolare immagini d'installazione

3.2.1 Definizione configurazione standard per tutti i tipi di sistema

3.2.2 Ripristino sistemi compromessi con configurazione standard

3.2.3 Procedure gestione cambiamenti per modifiche a configurazione standard

3.3.1 Immagini installazione memorizzate offline

3.3.2 Conservazione protetta immagini installazione (integrità/accesso protetto)

3.4.1 Eseguire amministrazione remota su connessioni protette (protocolli sicuri/canali protetti)

3.5.1 Verifica integrità file critici di sistema, eseguibili sistema/applicazioni, librerie, configurazioni

3.5.2 Verifica integrità file automatica e alert su alterazione

3.5.3 Cronologia modifica configurazione e identificazione autore

3.5.4 identificare alterazioni sospette sistema, permessi file/cartelle

3.6.1 Sistema centralizzato controllo automatico configurazioni

3.7.1 Strumenti per ripristino impostazioni configurazioni standard

Livello sicurezza Minimo | Livello sicurezza Standard | Livello sicurezza Alto

ABSC 4 (CSC 4) 1/2

Valutazione e correzione continua della vulnerabilità

4.1.1 Ricerca automatica vulnerabilità ad ogni modifica significativa della configurazione di tutti i sistemi in rete

4.1.2 Ricerca periodica vulnerabilità (frequenza commisurata complessità dell'infrastruttura)

4.1.3 Utilizzo SCAP (Security Content Automation Protocol) per validazione vulnerabilità basate sul codice e configurazione

4.2.1 Correlazione log di sistema - scansioni delle vulnerabilità

4.2.2 Verificare che i log registrino attività di scanning delle vulnerabilità

4.2.3 Verificare che i log registrino gli attacchi

4.3.1 Eseguire scansioni vulnerabilità locali/remote con account dedicato

4.3.2 Eseguire scansioni vulnerabilità da host/IP specifici

4.4.1 Aggiornare gli strumenti di scansione delle vulnerabilità

4.4.2 Registrazione a servizio che fornisce informazioni tempestive su nuove minacce/vulnerabilità e utilizzarle nelle scansioni

4.5.1 Installazione automatica patch/aggiornamenti per software/OS

4.5.2 Aggiornare sistemi separati dalla rete/air-gapped in base al loro livello di criticità

ABSC 4 (CSC 4) 2/2

Valutazione e correzione continua della vulnerabilità

4.6.1 Verifica che le scansioni siano eseguite con policy predefinite

4.7.1 Verifica risoluzione vulnerabilità emerse (patch, contromisure documentazione accettazione rischio)

4.7.2 Revisione periodica delle accettazioni dei rischi di vulnerabilità

4.8.1 Definizione piano gestione rischi | 4.8.2 Attribuire alle azioni per risoluzione vulnerabilità un livello di priorità in base al rischio

4.9.1 Misure alternative se non è possibile risolvere la vulnerabilità

4.10.1 Ambiente test per patch software non standard (xes. ad hoc)

ABSC 5 (CSC 5) 1/2

Uso appropriato dei privilegi di amministratore

- 5.1.1 Limitare privilegi di amministrazione ai soli utenti necessari
- 5.1.2 Utilizzo utenze amministrative solo quando necessario
- 5.1.3 Assegnare agli utenti amministratori solo i privilegi necessari
- 5.1.4 Log attività utenze amministrative e rilevare anomalie
- 5.2.1 Inventario utenze amministrative
- 5.2.2 Automazione inventario utenze amministrative e alert variazioni
- 5.3.1 Cambio credenziali amministrative predefinite dei dispositivi connessi in rete
- 5.4.1 Log aggiunta/soppressione utenza amministrativa
- 5.4.2 Alert aggiunta utenza amministrativa
- 5.4.3 Alert aumento privilegi utenza amministrativa
- 5.5.1 Log accessi falliti da utenze amministrative
- 5.6.1 Utilizzo sistemi di autenticazione a più fattori per tutti gli accessi amministrativi
- 5.7.1 Se l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali robuste (almeno 14 caratteri)
- 5.7.2 Impedire utilizzo credenziali amministrative deboli
- 5.7.3 Assicurarsi che credenziali delle utenze amministrative vengano sostitute con sufficiente frequenza (password aging)
- 5.7.4 Impedire riutilizzo credenziali utenze amministrative a breve distanza di tempo (password history)
- 5.7.5 Consentire modifica credenziali amministrative dopo un lasso di tempo sufficiente
- 5.7.6 Impedire riutilizzo credenziali amministrative prima di 6 mesi

Livello sicurezza Minimo | Livello sicurezza Standard | Livello sicurezza Alto

ABSC 5 (CSC 5) 2/2

Uso appropriato dei privilegi di amministratore

5.8.1 Impedire accesso diretto ai sistemi con utenze amministrative, obbligare gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi

5.9.1 Utilizzare per operazioni amministrative macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet

5.10.1 Credenziali distinte utenze privilegiate e non privilegiate degli amministratori

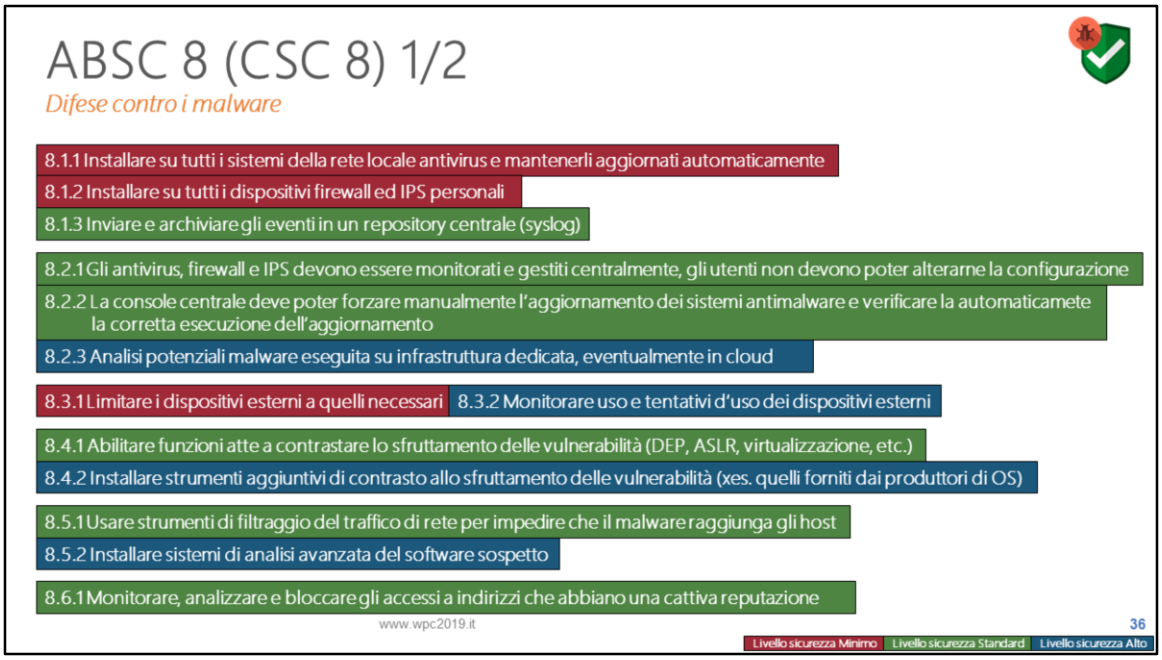
5.10.2 Tutte le utenze devono essere nominative e riconducibili ad una sola persona, in particolare quelle amministrative

5.10.3 Le utenze amministrative anonime («root», «administrator») devono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso

5.10.4 Evitare uso utenze amministrative locali quando sono disponibili utenze amministrative di livello più elevato (xes. dominio)

5.11.1 Conservare le credenziali amministrative garantendo disponibilità e riservatezza

5.11.2 Se si utilizzano certificati digitali per l'autenticazione, garantire adeguata protezione per le chiavi private



Data Execution Prevention (DEP)
Address Space Layout Randomization (ASLR)

ABSC 8 (CSC 8) 2/2

Difese contro i malware

8.7.1 Disattivare esecuzione automatica su dispositivi removibili | 8.7.2 Disattivare esecuzione automatica contenuti dinamici file (macro)

8.7.3 Disattivare apertura automatica mail | 8.7.4 Disattivare anteprima automatica contenuto file

8.8.1 Eseguire scansione anti-malware automatica alla connessione di supporti rimuovibili

8.9.1 Filtrare il contenuto delle mail prima raggiungano la casella del destinatario, prevedere anche l'impiego di antispam

8.9.2 Filtrare il contenuto del traffico web

8.9.3 Bloccare nelle email e traffico web i tipi di file non necessari e potenzialmente pericolosi

8.10.1 Utilizzare anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento

8.10.1 Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate

8.4.2 Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità (xes. quelli forniti dai produttori di OS)

ABSC 10 (CSC 10)

Copie di sicurezza

10.1.1 Effettuare almeno copia settimanale delle informazioni strettamente necessarie per il completo ripristino del sistema

10.1.2 Eseguire backup di OS, applicazioni e dati | 10.1.2 Eseguire backup multipli con strumenti diversi

10.2.1 Eseguire una verifica periodica delle copie tramite rispristino di prova

10.3.1 Assicurare la riservatezza delle copie di sicurezza mediante protezione fisica dei supporti o mediante cifratura, la codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud

10.4.1 Assicurare che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema per evitare che attacchi possano coinvolgere anche tutte le sue copie di sicurezza

ABSC 13 (CSC 13)

Protezione dei dati

13.1.1 Effettuare un'analisi dei dati per individuare quelli riservati (dati rilevanti) a cui applicare la protezione crittografica

13.2.1 Utilizzare la cifratura per dispositivi portatili e sistemi che contengono informazioni rilevanti

13.3.1 Monitorare e bloccare con strumenti automatici l'uso della crittografia non autorizzata sul traffico di rete uscente

13.4.1 Effettuare scansioni periodiche con sistemi automatici per rilevare sui server "data pattern" significativi per l'Amministrazione che evidenzino l'esistenza di dati rilevanti in chiaro

13.5.1 Implementare sistemi/configurazioni per impedire la scrittura di dati dispositivi esterni se questi non sono strettamente necessari

13.5.2 Gestire centralmente il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a proprietà univoche) cifrando i dati e mantendo una lista aggiornata dei dispositivi

13.6.1 Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare il flusso dei dati in rete e individuare anomalie

13.6.2 Registrare le anomalie del traffico di rete per consentire analisi off line

13.7.1 Monitorare il traffico uscente rilevando la crittografia non prevista

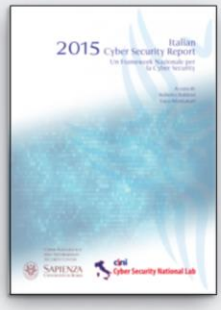
13.8.1 Bloccare il traffico da e verso url presenti in una blacklist

13.9.1 Assicurare che la copia autorizzata di un file mantenga le limitazioni di accesso della sorgente

Livello sicurezza Minimo | Livello sicurezza Standard | Livello sicurezza Alto


WPC19
Framework Nazionale per la Cybersecurity e la Data Protection
Normative regolamenti e indicazioni tecniche per la sicurezza ICT per PA e aziende private
OverNet EDUCATION
www.wpc2019.it
40

Overview



2013 → **2014** → **2015** → **2016** → **2017** → **2018** → **2019**

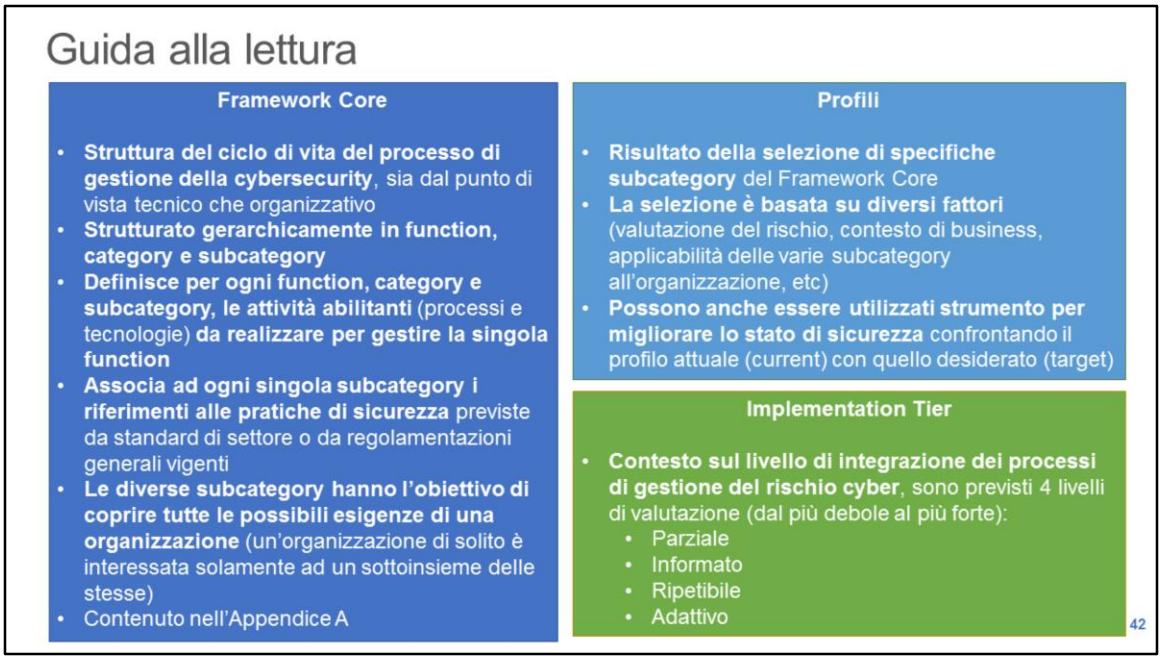
Strumento di supporto alle organizzazioni, ma non deve essere considerato uno strumento per il rispetto ai regolamenti vigenti

Aiuta le organizzazioni nel definire un percorso volto alla cybersecurity e alla protezione dei dati coerente con i regolamenti stessi

Per le organizzazioni che già implementano misure coerenti con il GDPR, **il Framework rappresenta un utile strumento per guidare le necessarie attività di monitoraggio**

https://www.cybersecurityframework.it/

41



una singola organizzazione è interessata solamente ad un sottoinsieme delle stesse

Framework Core

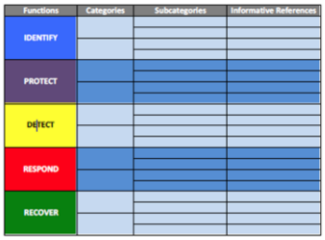
La function IDENTIFY è legata alla comprensione del contesto aziendale, degli asset che supportano i processi critici di business e dei relativi rischi associati

La function PROTECT è associata all'implementazione di quelle misure volte alla protezione dei processi di business e degli asset aziendali, indipendentemente dalla loro natura informatica

La function DETECT è associata alla definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica

La function RESPOND è associata alla definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato
L'obiettivo è contenere l'impatto determinato da un potenziale incidente di sicurezza informatica

La function RECOVER è associata alla definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente
L'obiettivo è garantire la resilienza dei sistemi e delle infrastrutture e, in caso di incidente, supportare il recupero tempestivo delle business operations



Informative Reference

Riferimenti che legano la singola subcategory alle pratiche di sicurezza note previste da standard di settore (ISO, SP800-53r4, COBIT-5, SANS20 e altri) o da regolamentazioni generali vigenti (Regolamento UE 2016/679 General Data Protection Regulation, Direttiva UE 2016/1148 NIS)

Tali riferimenti hanno principalmente uno scopo illustrativo e non devono essere interpretati come esaustivi

Versione 2.0 Febbraio 2019

Basata sul Cybersecurity Framework sviluppato dal National Institute of Standards and Technology (NIST) recentemente aggiornato alla versione 1.1

Sono stati **integrati i cambiamenti apportati dal NIST al Framework Core**, includendo elementi volti a considerare le problematiche di **sicurezza delle filiere di approvvigionamento** (supply chain) e ad approfondire la **sicurezza dei processi di autenticazione e gestione delle identità**

Include una serie di **nuovi elementi indirizzati a guidare la corretta gestione dei dati personali**, con specifico riferimento alla sicurezza degli stessi a fronte di possibili attacchi informatici

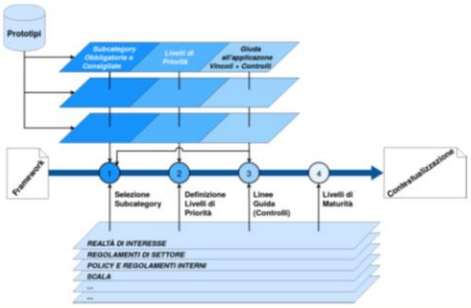
Introdotte **9 nuove subcategory e una nuova category** relative agli aspetti **legati alla data protection**

Introdotto un nuovo strumento per la contestualizzazione del Framework sotto forma di prototipi di contestualizzazione che permette di definire dei template applicabili in fase di contestualizzazione per integrare più facilmente nella stessa concetti legati a normative, regolamenti o best practice
http://tool.cybersecurityframework.it/

Guida all'uso – Contestualizzazione e implementazione

Contestualizzazione ad un ambito applicativo

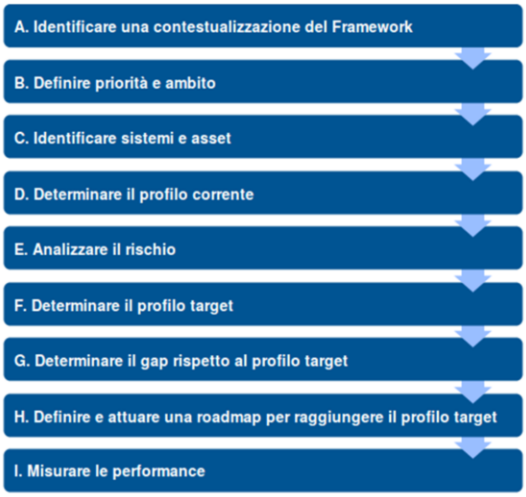
1. **Selezionare dell'elenco delle function, category, subcategory pertinenti** per l'organizzazione in base a tutti o alcuni elementi (settore produttivo, dimensione e dislocazione sul territorio, ecc.)
2. **Definire i livelli di priorità** per l'implementazione delle subcategory selezionate
3. **Definire delle linee guida** almeno per le subcategory a priorità alta
4. Specificare i livelli di maturità almeno per le subcategory a priorità alta



Implementazione di un prototipo in una contestualizzazione

1. Tutte le subcategory indicate come obbligatorie nel prototipo vengono selezionate nella contestualizzazione
2. La selezione nella contestualizzazione delle subcategory indicate come consigliate nel prototipo deve essere valutata in considerazione delle specifiche caratteristiche dell'ambito applicativo previsto per la contestualizzazione
3. Eventuali ulteriori vincoli sulla selezione delle subcategory documentati nella guida di applicazione del prototipo devono essere applicati
4. Per ogni subcategory selezionata a seguito dei precedenti passi deve essere indicato nella contestualizzazione un livello di priorità, preferibilmente almeno pari o superiore a quello indicato nel prototipo, tenendo conto di eventuali vincoli documentati nella guida di applicazione del prototipo
5. Gli eventuali controlli di sicurezza documentati nella guida di applicazione del prototipo possono essere integrati nelle linee guida all'applicazione della contestualizzazione

Guida all'uso – Applicazione



L'obiettivo principale del Framework è fornire alle organizzazioni interessate uno strumento di supporto al processo di gestione e trattamento del rischio cyber. È plausibile che in molte realtà si siano già avviati da tempo programmi di cybersecurity e siano già implementati standard per la data protection, in ragione dei quali l'introduzione del Framework è da intendersi non tanto per sostituire quanto già in essere, ma come ulteriore riferimento

Integrazione dei Controlli Essenziali

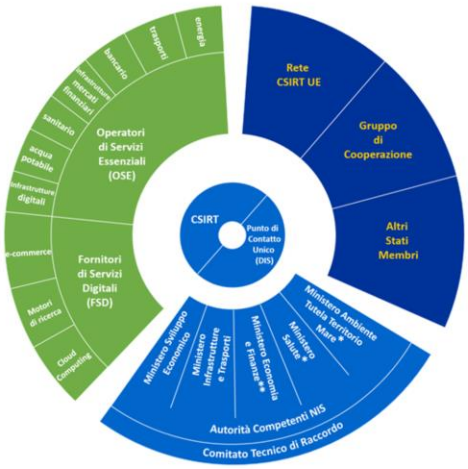
Tematiche		Controlli Essenziali di Cybersecurity
Inventario dispositivi e software	1	Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale.
	2	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc...) offerti da terze parti a cui si è registrati sono quelli strettamente necessari.
	3	Sono individuate le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti.
	4	È stato nominato un referente che sia responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici.
Governance	5	Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in tema di cybersecurity che risultino applicabili per l'azienda.
Protezione da malware	6	Tutti i dispositivi che lo consentono sono dotati di software di protezione (antivirus, antimalware, ecc...) regolarmente aggiornato.
Gestione password e account	7	Le password sono diverse per ogni account, della complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più sicuri offerti dal provider del servizio (es. autenticazione a due fattori).
	8	Il personale autorizzato all'accesso, remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri; l'accesso è opportunamente protetto; i vecchi account non più utilizzati sono disattivati.
	9	Ogni utente può accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza.

Tematiche		Controlli Essenziali di Cybersecurity
Formazione e consapevolezza	10	Il personale è adeguatamente sensibilizzato e formato sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego sicuro degli strumenti aziendali (es. riconoscere allegati e-mail, utilizzare solo software autorizzato, ...). I vertici aziendali hanno cura di predisporre per tutto il personale aziendale la formazione necessaria a fornire almeno le nozioni basilari di sicurezza.
Protezione dei dati	11	La configurazione iniziale di tutti i sistemi e dispositivi è svolta da personale esperto, responsabile per la configurazione sicura degli stessi. Le credenziali di accesso di default sono sempre sostituite.
	12	Sono eseguiti periodicamente backup delle informazioni e dei dati critici per l'azienda (identificati al controllo 3). I backup sono conservati in modo sicuro e verificati periodicamente.
Protezione delle reti	13	Le reti e i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (es: Firewall e altri dispositivi/software anti-intrusione).
Prevenzione e mitigazione	14	In caso di incidente (es. venga rilevato un attacco o un malware) vengono informati i responsabili della sicurezza e i sistemi vengono messi in sicurezza da personale esperto.
	15	Tutti i software in uso (inclusi i firmware) sono aggiornati all'ultima versione consigliata dal produttore. I dispositivi o i software obsoleti e non più aggiornabili sono dismessi.

***Rappresentano un insieme minimo di pratiche di sicurezza che non possono essere ignorate**; una base da cui deve partire un percorso di miglioramento progressivo che porti ad allinearsi con la metodologia di gestione della cybersecurity basata sul Framework Nazionale*


WPC19
Direttiva NIS
(Direttiva 2016/1148)
Normative regolamenti e indicazioni tecniche
per la sicurezza ICT per PA e aziende private
OverNet
EDUCATION
www.wpc2019.it
48

Direttiva NIS



Servizi interessati

Attori governativi NIS

Meccanismi della cooperazione europea

* più regioni e province autonome di Trento e di Bolzano

** in collaborazione con le autorità di vigilanza di settore, Banca d'Italia e Consob

Definisce le misure necessarie per conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi

Adottata in Italia con il Decreto Legislativo del 18 maggio 2018, n.65 (G.U. n. 132 del 9 giugno 2018) che ha recepito nell'ordinamento nazionale la Direttiva UE 2016/1148 (Direttiva NIS)

Il decreto si applica agli Operatori di Servizi Essenziali (OSE) e ai Fornitori di Servizi Digitali (FSD)

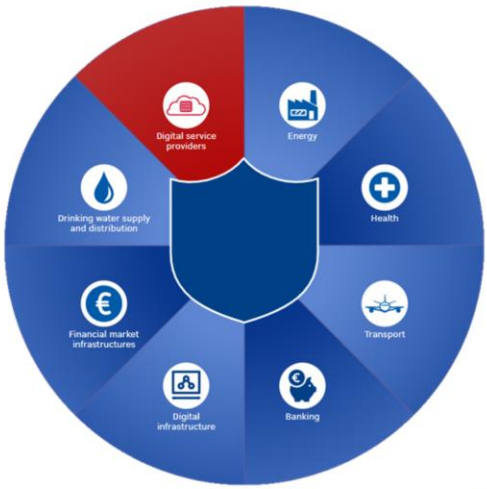
NIS Directive tool: https://www.enisa.europa.eu/topics/nis-directive/nis-visualtool

Obblighi degli OSE e degli FSD

Adottare **misure tecniche e organizzative adeguate e proporzionate** alla **gestione dei rischi**

Prevenire e minimizzare l'impatto degli incidenti a carico della sicurezza delle reti e dei sistemi informativi, al fine di assicurare la continuità del servizio

Notificare, senza ingiustificato ritardo, gli incidenti che hanno un **impatto rilevante**, rispettivamente sulla continuità e sulla fornitura del servizio, al *Computer Security Incident Response Team* (CSIRT) italiano, informandone anche l'Autorità competente NIS di riferimento.



https://www.csirt-ita.it/nis.html

Obblighi degli FSD

Applicare le prescrizioni dettate dal decreto di recepimento a partire dal 24 giugno 2018, data di entrata in vigore del provvedimento, **valutando la rilevanza degli incidenti sulla base dei criteri e delle soglie indicati nel Regolamento (UE) 2018/151 del 30 gennaio 2018**
https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018R0151&from=IT

Un incidente a carico di un FSD è rilevante se si verifica almeno una delle seguenti condizioni:

- **Indisponibilità** del servizio fornito **per oltre 5.000.000 ore utente**
- **Perdita di integrità, autenticità o riservatezza** dei dati **per oltre 100.000 utenti dell'UE**
- **Rischio per la sicurezza e/o l'incolumità pubblica**, o in termini di perdite di vite umane
- **Danni materiali superiori a 1.000.000 di EUR per almeno un utente nell'UE**

https://www.csirt-ita.it/nis.html

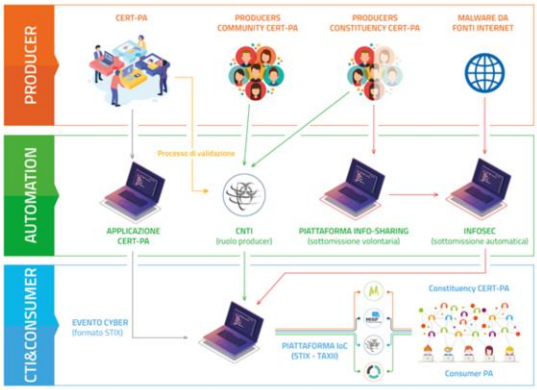
Autorità competenti NIS

Autorità competenti NIS	Ambito di competenza
Ministero dello sviluppo economico	Settore dell'energia – Sottosettori energia elettrica, gas e petrolio
	Settore delle infrastrutture digitali
	Servizi digitali
Ministero delle infrastrutture e dei trasporti	Settore dei trasporti – Sottosettori trasporto aereo, trasporto ferroviario, trasporto per vie d'acqua e trasporto su strada
Ministero dell'economia e delle finanze in collaborazione con Banca d'Italia e Consob Settore bancario	Settore bancario
	Settore delle infrastrutture dei mercati finanziari
Ministero della salute, Regioni e Province autonome di Trento e di Bolzano (direttamente o per il tramite delle Autorità sanitarie territorialmente competenti)	Settore sanitario
Ministero dell'ambiente e della tutela del territorio e del mare, Regioni e Province autonome di Trento e di Bolzano (direttamente o per il tramite delle Autorità territorialmente competenti)	Settore della fornitura e distribuzione di acqua potabile

Piattaforma Nazionale per il contrasto agli attacchi informatici

Iniziativa avviata con l'approvazione e la supervisione del Nucleo per la sicurezza cibernetica (NSC) costituito presso il Dipartimento delle informazioni per la sicurezza

Favorire tra le pubbliche amministrazioni lo scambio automatizzato di informazioni (infosharing) che interessano eventi di rischio cibernetico, grazie a standard tecnici, linguaggio comune e soluzioni open source, per facilitarle nel trattamento e nella prevenzione degli attacchi informatici e, di conseguenza, nell'applicazione del Decreto Legislativo 18 maggio 2018 n.65 "direttiva NIS"



https://www.cert-pa.it/notizie/il-cert-pa-avvia-la-fase-pilota-della-piattaforma-nazionale-per-il-contrasto-agli-attacchi-informatici/


WPC19
Cybersecurity Act (Regolamento 2019/881)
Normative regolamenti e indicazioni tecniche per la sicurezza ICT per PA e aziende private
OverNet EDUCATION
www.wpc2019.it
54

Cybersecurity Act

Il testo definitivo del **Regolamento UE 2019/881** (Cybersecurity Act) è stato pubblicato sulla Gazzetta ufficiale dell'Unione europea **L 151/15 del 7 giugno 2019** https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019R0881&from=IT

Il provvedimento è **entrato in vigore il 27 giugno 2019**, trattandosi di un Regolamento è diventato immediatamente esecutivo in tutti gli Stati membri senza necessità di interventi attuativi da parte dei legislatori nazionali

Il Cybersecurity Act prevede la **certificazione delle infrastrutture critiche**, comprese le reti energetiche, l'acqua e i sistemi bancari, oltre a prodotti, processi e servizi, **e garantisce che soddisfino gli standard di sicurezza informatica**

Mandato permanente e maggiori risorse per l'Agenzia europea per la sicurezza informatica, l'ENISA

L'ENISA oltre a svolgere i suoi consueti compiti di consulenza tecnica, svolgerà anche attività di supporto alla gestione operativa degli incidenti informatici da parte degli Stati membri

Con la decisione presa il 12 marzo 2019, inoltre, il Parlamento europeo ha affidato all'ENISA un ruolo di primo piano nella gestione del sistema di certificazione introdotto dal Cybersecurity Act

Il Cybersecurity Act non istituisce schemi di certificazione direttamente operativi, ma crea un "quadro" per l'istituzione di schemi europei per la certificazione di prodotti e servizi digitali

https://www.enisa.europa.eu/topics/standards

Articolo 51

Obiettivi di sicurezza dei sistemi europei di certificazione della cibersicurezza

I sistemi europei di certificazione della cibersicurezza sono progettati per conseguire, se del caso, almeno i seguenti obiettivi di sicurezza:

a) proteggere i dati conservati, trasmessi o altrimenti trattati dall'archiviazione, dal trattamento, dall'accesso o dalla divulgazione accidentali o non autorizzati durante l'intero ciclo di vita del prodotto TIC, del servizio TIC o del processo TIC;

b) proteggere i dati conservati, trasmessi o altrimenti trattati dalla distruzione, dalla perdita o dall'alterazione accidentali o non autorizzate, oppure dalla mancanza di disponibilità durante l'intero ciclo di vita del prodotto TIC, del servizio TIC o del processo TIC;

c) le persone, i programmi o le macchine autorizzati devono poter accedere esclusivamente ai dati, ai servizi o alle funzioni per i quali dispongono dei diritti di accesso;

d) individuare e documentare le dipendenze e vulnerabilità note;

e) registrare a quali dati, servizi o funzioni è stato effettuato l'accesso e quali sono stati utilizzati o altrimenti trattati, in quale momento e da chi;

f) fare in modo che si possa verificare quali sono i dati, i servizi o le funzioni a cui è stato effettuato l'accesso, che sono stati utilizzati o altrimenti trattati, in quale momento e da chi;

g) verificare che i prodotti TIC, i servizi TIC e i processi TIC non contengano vulnerabilità note;

h) ripristinare la disponibilità e l'accesso ai dati, ai servizi e alle funzioni in modo tempestivo in caso di incidente fisico o tecnico;

i) i prodotti TIC, i servizi TIC e i processi TIC devono essere sicuri fin dalla progettazione e per impostazione predefinita;

j) il software e l'hardware dei prodotti TIC, dei servizi TIC e dei processi TIC devono essere aggiornati, non contenere vulnerabilità pubblicamente note e devono disporre di meccanismi per effettuare aggiornamenti protetti.

Protezione dati | Autorizzazione accesso | Gestione Vulnerabilità | Registrazione utilizzo | Aggiornamento

Articolo 52 Paragrafi 1,2,3,4,5

Livelli di affidabilità dei sistemi europei di certificazione della cibersicurezza

1. I sistemi europei di certificazione della cibersicurezza possono specificare per i prodotti TIC, i servizi TIC e i processi TIC uno o più dei seguenti livelli di affidabilità: «di base», «sostanziale» o «elevato». Il livello di affidabilità è commisurato al livello del rischio associato al previsto uso del prodotto TIC, servizio TIC o processo TIC, in termini di probabilità e impatto di un incidente.
2. I certificati europei di cibersicurezza e le dichiarazioni UE di conformità si riferiscono a qualsiasi livello di affidabilità specificato nel sistema europeo di certificazione della cibersicurezza nell'ambito del quale si rilascia il certificato europeo di cibersicurezza o la dichiarazione UE di conformità.
3. I requisiti di sicurezza corrispondenti a ogni livello di affidabilità sono indicati nel sistema europeo di certificazione della cibersicurezza pertinente, comprese le corrispondenti funzionalità di sicurezza e il rigore e la specificità corrispondenti della valutazione a cui deve essere sottoposto il prodotto TIC, servizio TIC o processo TIC.
4. Il certificato o la dichiarazione UE di conformità si riferiscono a specifiche tecniche, norme e procedure ad esso connesse, tra cui i controlli tecnici, il cui obiettivo è ridurre il rischio di incidenti di cibersicurezza, o prevenirli
5. Un certificato europeo di cibersicurezza o una dichiarazione UE di conformità che si riferisca al livello di affidabilità «di base» assicura che i prodotti TIC, i servizi TIC e i processi TIC per i quali sono rilasciati tale certificato o tale dichiarazione UE di conformità rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo i rischi di base noti di incidenti e attacchi informatici. Le attività di valutazione da intraprendere comprendono almeno un riesame della documentazione tecnica. Qualora tale riesame non sia appropriato, si ricorre ad attività di valutazione sostitutive di effetto equivalente.

Livelli di affidabilità del prodotto (= livello di rischio)

Livelli di affidabilità «di base»

Articolo 52 Paragrafi 6,7,8

Livelli di affidabilità dei sistemi europei di certificazione della cibersicurezza

6. **Un certificato europeo di cibersicurezza che si riferisca al livello di affidabilità «sostanziale» assicura che i prodotti TIC, servizi TIC e processi TIC** per i quali è rilasciato tale certificato rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e **sono stati valutati a un livello inteso a ridurre al minimo i rischi noti connessi alla cibersicurezza e i rischi di incidenti e di attacchi informatici causati da soggetti dotati di abilità e risorse limitate**. Le attività di valutazione da intraprendere comprendono almeno le seguenti: un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note e un test per dimostrare che i prodotti TIC, i servizi TIC o i processi TIC attuano correttamente le necessarie funzionalità di sicurezza. Qualora tali attività di valutazione non siano appropriate, si ricorre ad attività di valutazione sostitutive di effetto equivalente.
7. **Un certificato europeo di cibersicurezza che si riferisca al livello di affidabilità «elevato» assicura che i prodotti TIC, i servizi TIC e i processi TIC** per i quali è rilasciato tale certificato rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e **sono stati valutati a un livello inteso a ridurre al minimo il rischio di attacchi informatici avanzati commessi da attori che dispongono di abilità e risorse significative**. Le attività di valutazione da intraprendere comprendono almeno le seguenti: un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note, un test per dimostrare che i prodotti TIC, i servizi TIC o i processi TIC attuano correttamente le necessarie funzionalità di sicurezza, allo stato tecnologico più avanzato, e una valutazione della loro resistenza agli attacchi commessi da soggetti qualificati mediante test di penetrazione. Qualora tali attività di valutazione non siano appropriate, si ricorre ad attività sostitutive di effetto equivalente.
8. **I sistemi europei di certificazione della cibersicurezza possono precisare vari livelli di valutazione in funzione del rigore e della specificità della metodologia di valutazione utilizzata**. Ciascun livello di valutazione corrisponde a uno dei livelli di affidabilità ed è definito da un'idonea combinazione di componenti dell'affidabilità.

Livelli di affidabilità «sostanziale» | Livelli di affidabilità «elevato»

WPC19

Q&A

Contatti

OverNet Education

- Info@OverNetEducation.it
- www.OverNetEducation.it
- Rozzano (MI) +39 02 365738
- Bologna +39 051 269911

- www.wpc-overneteducation.it
- #wpc19it