Giornata di Studio

5° SEMINARIO NAZIONALE ITS NEL TPL: Mobility as a Service e Approfondimenti Cybersecurity

ADEMPIMENTI NORMATIVI E CHECK-LIST

Andrea Vitiello
Supporto R&S e Innovazione
Ente Autonomo Volturno

EAV IN VIAGGIO DAL 1889

Genova 3 maggio 2023

In qualità di Provider asstra service

con il supporto di AMT MOBILITÀ E INNOVAZIONE, asstra IMPRESE IN MOVIMENTO

Quali argomenti affronteremo?

- **Adempimenti normativi**
  Le principali direttive, normative e regolamenti che hanno definito negli anni il perimetro operativo del settore della sicurezza cibernetica, sia nell'ambito dell'Unione Europea che in quello nazionale italiano.

- **Check-list cybersecurity per le aziende del TPL**
  Riferimento operativo comune di misure tecniche ed organizzative per le aziende del TPL, con la finalità di verificare lo stato di protezione contro le minacce informatiche e tracciare di conseguenza un percorso di miglioramento aziendale.

Panorama normativo europeo e nazionale (1/2)

Unione Europea		Italia	
Anno		**Anno**	
2016	**Direttiva UE 2016/1148** (06/07/2016) c.d. Direttiva NIS (Network and Information Security)		
		2017	**Circolare AgID n.2** (18/04/2017) *"Misure Minime di sicurezza ICT per le PA"*
		2018	**D.Lgs. 65** (18/05/2018) Recepimento Direttiva NIS
2019	**Regolamento UE 2019/881** (17/04/2019)		
		2019	**D.L. 105** (21/09/2019) *"Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica"*

Panorama normativo europeo e nazionale (2/2)

		2021	**D.L. 82 (14/06/2021)**
		2021	**Legge 109** (04/08/2021) (conversione in legge del D.L. 82) *"Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale"*
		2022	**Protocollo d'intesa** (26/01/2022) (tra l'Autorità Garante per la protezione dei dati personali e il Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale)
2022	**Direttiva UE 2022/2555** (14/12/2022) c.d. Direttiva NIS2		

Direttiva UE 2016/1148 – NIS (1/3)

La direttiva NIS, adottata dall'Unione Europea nel 2016 e recepita in Italia dal Decreto Legislativo del 18 maggio 2018, stabilisce i **requisiti minimi per la sicurezza** delle reti e dei sistemi informativi nell'UE.

Si applica agli operatori di servizi essenziali (OSE) e ai fornitori di servizi digitali (FSD). I primi sono soggetti pubblici o privati che prestano servizi la cui interruzione avrebbe un impatto significativo sulla società o sull'ambiente (settori energia, trasporti ferroviari, trasporti aerei, acqua potabile e gestione delle acque reflue, sanità). I secondi sono aziende che offrono servizi basati su tecnologie digitali (internet, cloud computing) e forniscono servizi digitali ai consumatori, come lo shopping online o il banking online.

Direttiva UE 2016/1148 – NIS (2/3)

Ciascuno Stato membro ha la possibilità di identificare i propri operatori di servizi essenziali e fornitori di servizi digitali e di applicare i requisiti della direttiva NIS in modo da garantire un livello adeguato di sicurezza delle informazioni.

La direttiva si basa su tre pilastri:

- **prevenzione**: gli operatori di servizi essenziali e i fornitori di servizi digitali devono mettere in atto misure per prevenire gli attacchi informatici;
- **rilevamento**: gli stessi devono essere in grado di individuare tempestivamente gli attacchi informatici;
- **mitigazione**: essi devono essere in grado di ripristinare rapidamente i propri servizi in caso di attacco informatico.

Direttiva UE 2016/1148 – NIS (3/3)

Ad operatori di servizi essenziali e forntori di servizi digitali sono richiesti alcuni obblighi, tra i quali:

- progettare **misure tecniche** capaci di gestire i rischi informatici e designare un responsabile della sicurezza delle informazioni;
- puntare sulla **prevenzione** di incidenti che violino la sicurezza delle proprie reti informatiche;
- contenere i danni di eventuali attacchi e **garantire la continuità dei servizi**;
- **notificare alle autorità competenti**, entro 24 ore, gli incidenti che minano la continuità e la fornitura dei servizi o comportino la divulgazione di dati sensibili. Poi, entro le 72 ore, inviare un report dettagliato di quanto avvenuto.

Perché aggiornare la Direttiva NIS?

- Il problema più importante riguardava le normative di recepimento: poiché la Direttiva NIS non sanciva espressamente i criteri utili all'individuazione dei c.d. "servizi essenziali", il panorama definitorio rappresentato dagli atti di recepimento degli Stati membri appariva non omogeneo, dunque in contrasto con il senso stesso della Direttiva, ossia armonizzare la disciplina degli Stati membri in materia di cybersecurity;
- la pandemia ha dimostrato come persistessero criticità notevoli in relazione alla cybersecurity, soprattutto nell'ambito dello smart working, dove l'impiego degli strumenti informatici è, per definizione, diffuso e lontano dalla sorveglianza del responsabile dell'azienda;
- negli ultimi anni si è assistito ad un aumento vertiginoso di attacchi informatici.

Direttiva UE 2022/2555 – NIS2

La Direttiva NIS2 persegue i medesimi obiettivi a cui mirava la Direttiva NIS, rispetto alla quale le modifiche riguardano i soggetti interessati, gli obblighi, le sanzioni e, più in generale, l'approccio che deve essere tenuto nell'adempimento di quanto richiesto dal testo normativo. Prevede inoltre obblighi di vigilanza ed esecuzione in capo agli Stati membri e norme in materia di condivisione delle informazioni sulla cybersecurity tra le varie Autorità europee.

La novità principale della Direttiva NIS2 è il suo ambito di applicazione. Le nuove disposizioni normative, oltre ad essere applicabili ai settori originariamente previsti dalla Direttiva, sono applicabili anche ad un novero di società più ampio e meglio definito.

Il termine per il recepimento nazionale è fissato al 18 ottobre 2024.

Check-list cybersecurity per le aziende del TPL (1/10)

Questa check-list inerente agli adempimenti in ambito di sicurezza informatica è stata creata per le aziende del TPL, partendo dal documento allegato alla Circolare AGID n.2 18/04/2017 *"Modulo di Implementazione delle misure minime di sicurezza per le PA"*, modello che fornisce un ausilio per determinare il livello di copertura prodotto dalle misure poste in essere dalle amministrazioni. Rispetto al documento originario, la check-list che segue riporta solo le misure corrispondenti al livello minimo e al livello standard previsti nell'applicazione delle misure minime per contrastare le minacce informatiche più frequenti, tralasciando il livello avanzato.

Assimilando pertanto le aziende di TPL alle PA, si considera il livello minimo come il livello che deve necessariamente essere raggiunto, mentre il livello standard è quello che ogni azienda deve considerare come base di riferimento in termini di sicurezza.

Check-list cybersecurity per le aziende del TPL (2/10)

ACRONIMO	DESCRIZIONE
ABSC	AgID Basic Security Control
CCSC	Center for Critical Security Control
CSC	Critical Security Control

LIVELLI PREVISTI DI APPLICAZIONE DELLE MISURE	
M	Minimo: livello al quale ogni PA deve essere o rendersi conforme
S	Standard: livello base di riferimento per la maggior parte dei casi

Check-list cybersecurity per le aziende del TPL (3/10)

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso.

ABSC_ID			Livello	Descrizione
1	1	1	M	**Implementare un inventario delle risorse attive correlato a quello ABSC 1.4.**
		2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico.
	2	1	S	Implementare il "logging" delle operazione del server DHCP.
		2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.
	3	1	M	**Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.**
		2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.
	4	1	M	**Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.**
		2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.

Check-list cybersecurity per le aziende del TPL (4/10)

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione.

ABSC_ID			Livello	Descrizione
2	1	1	M	**Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.**
	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.
		2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).
	3	1	M	**Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.**
		2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.

Check-list cybersecurity per le aziende del TPL (5/10)

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.

ABSC_ID			Livello	Descrizione
3	1	1	M	**Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.**
		2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.
	2	1	M	**Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.**
		2	M	**Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.**
		3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.
	3	1	M	**Le immagini d'installazione devono essere memorizzate offline.**
		2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.
	4	1	M	**Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).**
	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.

Check-list cybersecurity per le aziende del TPL (6/10)

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

ABSC_ID			Livello	Descrizione
4	1	1	M	**Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.**
		2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.
	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.
		2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità
		3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.
	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.
		2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.
	4	1	M	**Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.**
		2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione
	5	1	M	**Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.**
		2	M	**Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.**
	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.
	7	1	M	**Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.**
		2	S	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.
	8	1	M	**Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (es. server esposti, server interni, PdL, portatili, etc.).**
		2	M	**Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.**
	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.
	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.

Check-list cybersecurity per le aziende del TPL (7/10)

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

ABSC_ID			Livello	Descrizione
5	1	1	M	**Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.**
		2	M	**Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.**
		3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.
	2	1	M	**Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.**
	3	1	M	**Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.**
	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.
		2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.
		3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.
	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.
	7	1	M	**Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).**
		2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.
		3	M	**Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).**
		4	M	**Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).**
		5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.
		6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.
	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.
	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.
	10	1	M	**Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.**
		2	M	**Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.**
		3	M	**Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono 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.**
		4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).
	11	1	M	**Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.**
		2	M	**Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.**

Check-list cybersecurity per le aziende del TPL (8/10)

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.

ABSC_ID			Livello	Descrizione
8	1	1	M	**Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.**
		2	M	**Installare su tutti i dispositivi firewall ed IPS personali.**
		3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.
	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.
		2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.
	3	1	M	**Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.**
	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.
	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.
	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.
	7	1	M	**Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.**
		2	M	**Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.**
		3	M	**Disattivare l'apertura automatica dei messaggi di posta elettronica.**
		4	M	**Disattivare l'anteprima automatica dei contenuti dei file.**
	8	1	M	**Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.**
	9	1	M	**Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.**
		2	M	**Filtrare il contenuto del traffico web.**
		3	M	**Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).**
	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.
	11	1	S	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.

Check-list cybersecurity per le aziende del TPL (9/10)

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.

ABSC_ID			Livello	Descrizione
10	1	1	M	**Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.**
	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.
	3	1	M	**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.**
	4	1	M	**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.**

Check-list cybersecurity per le aziende del TPL (10/10)

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti.

ABSC_ID			Livello	Descrizione
13	1	1	M	**Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica.**
	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti.
	8	1	M	**Bloccare il traffico da e verso url presenti in una blacklist.**

Giornata di Studio

5° SEMINARIO NAZIONALE ITS NEL TPL: Mobility as a Service e Approfondimenti Cybersecurity

✷ *Grazie per la cortese attenzione* ✷

Andrea Vitiello
Supporto R&S e Innovazione
Ente Autonomo Volturno

EAV IN VIAGGIO DAL 1889

Genova 3 maggio 2023

In qualità di Provider asstra service

con il supporto di AMT MOBILITÀ E INNOVAZIONE, asstra IMPRESE IN MOVIMENTO