Solo i testi UNECE originali hanno efficacia giuridica ai sensi del diritto internazionale pubblico. Lo status e la data di entrata in vigore del presente regolamento devono essere controllati nell'ultima versione del documento UNECE TRANS/WP.29/343, reperibile al seguente indirizzo: https://unece.org/status-1958-agreement-and-annexed-regulations

Regolamento n. 155 della Commissione economica per l'Europa delle Nazioni Unite (UNECE) — Disposizioni uniformi relative all'omologazione dei veicoli per quanto riguarda la cibersicurezza e i sistemi di gestione della cibersicurezza [2025/5]

Comprendente tutti i testi validi fino a:

supplemento 3 alla versione originale del regolamento — Data di entrata in vigore: 10 gennaio 2025

Il presente documento è un semplice strumento di documentazione. I testi facenti fede e giuridicamente vincolanti sono i seguenti:

— ECE/TRANS/WP.29/2020/79 (quale modificato da ECE/TRANS/WP.29/2020/94 e ECE/TRANS/WP.29/2020/97)

— ECE/TRANS/WP.29/2022/54

— ECE/TRANS/WP.29/2023/70 e

— ECE/TRANS/WP.29/2024/55

INDICE

Regolamento

1. Ambito di applicazione
2. Definizioni
3. Domanda di omologazione
4. Marcature
5. Omologazione
6. Certificato di conformità del sistema di gestione della cibersicurezza
7. Specifiche
8. Modifica del tipo di veicolo ed estensione dell'omologazione
9. Conformità della produzione
10. Sanzioni in caso di non conformità della produzione
11. Cessazione definitiva della produzione
12. Nomi e indirizzi dei servizi tecnici responsabili delle prove di omologazione e delle autorità di omologazione

Allegati

1 Scheda informativa

2 Notifica

3 Esempio di marchio di omologazione

4 Modello di certificato di conformità del CSMS

5 Elenco delle minacce e delle misure di attenuazione corrispondenti

1. Ambito di applicazione

1.1. Il presente regolamento si applica, per quanto riguarda la cibersicurezza, ai veicoli delle categorie L, M, N e O, se muniti di almeno una centralina elettronica.

1.2. Il presente regolamento lascia impregiudicati gli altri regolamenti ONU, le normative regionali o nazionali che disciplinano l'accesso di parti autorizzate al veicolo, ai suoi dati, alle sue funzioni e alle sue risorse, nonché le condizioni di tale accesso. Esso non pregiudica inoltre l'applicazione della normativa nazionale e regionale in materia di privacy e protezione delle persone fisiche con riguardo al trattamento dei loro dati personali.

1.3. Il presente regolamento lascia impregiudicati altri regolamenti ONU o normative nazionali o regionali che disciplinano lo sviluppo e l'installazione/integrazione in sistemi di componenti e pezzi di ricambio, fisici e digitali, per quanto riguarda la cibersicurezza.

2. Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

2.1. "*tipo di veicolo*": veicoli che non presentano differenze per quanto riguarda almeno gli elementi essenziali seguenti:

a) la designazione del tipo di veicolo indicata dal costruttore;

b) aspetti essenziali dell'architettura elettrica/elettronica e delle interfacce esterne per quanto riguarda la cibersicurezza;

2.2. "*cibersicurezza*": la condizione in cui i veicoli stradali e le loro funzioni sono protetti da minacce informatiche nei confronti dei componenti elettrici o elettronici;

2.3. "*sistema di gestione della cibersicurezza (CSMS)*": approccio sistematico basato sul rischio che definisce i processi organizzativi, le responsabilità e la governance per il trattamento dei rischi associati alle minacce informatiche nei confronti dei veicoli e per la protezione degli stessi dagli attacchi informatici;

2.4. "*sistema*": un insieme di componenti e/o sottosistemi che svolge una o più funzioni;

2.5. "*fase di sviluppo*": il periodo che precede l'omologazione di un tipo di veicolo;

2.6. "*fase di produzione*": la durata della produzione di un tipo di veicolo;

2.7. "*fase di post-produzione*": il periodo in cui un tipo di veicolo non è più prodotto fino al termine del ciclo di vita di tutti i veicoli di tale tipo. Durante questa fase i veicoli conformi a uno specifico tipo di veicolo saranno operativi ma non saranno più prodotti. La fase si conclude quando non vi sono più veicoli operativi di tale specifico tipo di veicolo;

2.8. "*misura di attenuazione*": una misura che riduce il rischio;

2.9. "*rischio*": la possibilità che una data minaccia sfrutti le vulnerabilità di un veicolo arrecando in tal modo danno all'organizzazione o a un individuo;

2.10. "*valutazione del rischio*": l'intero processo di individuazione, riconoscimento e descrizione dei rischi (identificazione dei rischi), volto a comprendere la natura del rischio e a determinare il livello di rischio (analisi dei rischi), e di confronto dei risultati dell'analisi dei rischi con i criteri di rischio allo scopo di determinare se il rischio e/o la sua entità siano accettabili o tollerabili (valutazione dei rischi);

2.11. "*gestione del rischio*": attività coordinate al fine di dirigere e controllare un'organizzazione per quanto riguarda il rischio;

2.12. "*minaccia*": la causa potenziale di un incidente indesiderato che può danneggiare un sistema, un'organizzazione o una persona;

2.13. "*vulnerabilità*": una debolezza in un elemento o in una misura di attenuazione che può essere sfruttata da una o più minacce.

3. Domanda di omologazione

3.1. La domanda di omologazione di un tipo di veicolo per quanto riguarda la cibersicurezza deve essere presentata dal costruttore del veicolo o da un suo mandatario debitamente accreditato.

3.2. La domanda deve essere accompagnata dai documenti indicati nel seguito, in triplice copia, e dalle informazioni seguenti:

3.2.1. descrizione del tipo di veicolo per quanto riguarda gli elementi specificati nell'allegato 1 del presente regolamento;

3.2.2. nei casi in cui le informazioni sono coperte da diritti di proprietà intellettuale o costituiscono un know-how specifico del costruttore o dei suoi fornitori, il costruttore o i suoi fornitori devono mettere a disposizione informazioni sufficienti per effettuare correttamente i controlli di cui al presente regolamento. Tali informazioni devono essere trattate in via riservata;

3.2.3. il certificato di conformità del CSMS ai sensi del punto 6 del presente regolamento.

3.3. La documentazione deve essere messa a disposizione in due parti:

a) il fascicolo di documentazione ufficiale per l'omologazione, contenente il materiale specificato nell'allegato 1, che deve essere fornito all'autorità di omologazione o al suo servizio tecnico al momento della presentazione della domanda di omologazione. Tale fascicolo di documentazione deve essere utilizzato dall'autorità di omologazione o dal suo servizio tecnico come riferimento di base per il processo di omologazione. L'autorità di omologazione o il suo servizio tecnico devono garantire che tale fascicolo di documentazione resti disponibile per almeno 10 anni a decorrere dalla cessazione definitiva della produzione del tipo di veicolo;

b) il costruttore può conservare materiale supplementare relativo alle prescrizioni del presente regolamento, ma questo deve essere messo a disposizione per l'ispezione al momento dell'omologazione. Il costruttore deve garantire che qualsiasi materiale messo a disposizione per l'ispezione al momento dell'omologazione resti disponibile per un periodo di almeno 10 anni a decorrere dalla cessazione definitiva della produzione del tipo di veicolo.

4. Marcatura

4.1. Su ciascun veicolo conforme a un tipo di veicolo omologato a norma del presente regolamento deve essere apposto, in evidenza e in un punto di facile accesso specificato nella scheda di omologazione, un marchio di omologazione internazionale composto da:

4.1.1. un cerchio al cui interno è iscritta la lettera "E" seguita dal numero distintivo del paese che ha rilasciato l'omologazione;

4.1.2. il numero del presente regolamento, seguito dalla lettera "R", da un trattino e dal numero di omologazione, posti a destra del cerchio di cui al precedente punto 4.1.1.

4.2. Se nel paese che ha rilasciato l'omologazione a norma del presente regolamento il veicolo è conforme a un tipo di veicolo omologato a norma di altri regolamenti allegati all'accordo, non è necessario ripetere il simbolo di cui al punto 4.1.1; in tal caso, il regolamento, i numeri di omologazione e i simboli supplementari di tutti i regolamenti a norma dei quali è stata rilasciata l'omologazione, nel paese che l'ha rilasciata a norma del presente regolamento, devono essere incolonnati verticalmente a destra del simbolo di cui al punto 4.1.1.

4.3. Il marchio di omologazione deve essere chiaramente leggibile e indelebile.

4.4. Il marchio di omologazione deve essere posto sulla targhetta del costruttore, o in prossimità della stessa.

4.5. L'allegato 3 del presente regolamento riporta alcuni esempi di marchi di omologazione.

5. Omologazione

5.1. Le autorità di omologazione devono rilasciare, se del caso, l'omologazione per quanto riguarda la cibersicurezza solo ai tipi di veicolo che soddisfano le prescrizioni del presente regolamento.

5.1.1. L'autorità di omologazione o il servizio tecnico devono verificare, mediante controlli documentali, che il costruttore del veicolo abbia adottato le misure pertinenti per il tipo di veicolo al fine di:

a) raccogliere e verificare le informazioni richieste a norma del presente regolamento lungo la catena di approvvigionamento in modo da dimostrare che i rischi connessi ai fornitori sono individuati e gestiti;

b) documentare la valutazione del rischio (effettuata durante la fase di sviluppo o in maniera retrospettiva), i risultati delle prove e le misure di attenuazione applicate al tipo di veicolo, comprese le informazioni di progettazione a sostegno della valutazione del rischio;

c) attuare adeguate misure di cibersicurezza nella progettazione del tipo di veicolo;

d) rilevare e rispondere a possibili attacchi alla cibersicurezza;

e) registrare dati in un log per favorire l'individuazione di attacchi informatici e disporre di capacità di trattamento dei dati che consentano di analizzare gli attacchi informatici tentati o riusciti.

5.1.2. L'autorità di omologazione o il servizio tecnico devono verificare, mediante prove su un veicolo del tipo in questione, che il costruttore del veicolo abbia attuato le misure di cibersicurezza da esso documentate. Le prove devono essere eseguite dall'autorità di omologazione o dal servizio tecnico stesso o in collaborazione con il costruttore del veicolo mediante campionamento. Il campionamento deve essere incentrato, a titolo non esaustivo, sui rischi che sono giudicati elevati in fase di valutazione del rischio.

5.1.3. L'autorità di omologazione o il servizio tecnico devono rifiutarsi di rilasciare l'omologazione per quanto riguarda la cibersicurezza se il costruttore del veicolo non ha soddisfatto una o più prescrizioni di cui al punto 7.3, in particolare:

a) il costruttore del veicolo non ha effettuato l'esauriente valutazione del rischio di cui al punto 7.3.3; ciò include la mancata considerazione da parte del costruttore di tutti i rischi connessi alle minacce di cui all'allegato 5, parte A;

b) il costruttore del veicolo non ha protetto il tipo di veicolo dai rischi individuati nella valutazione del rischio da lui stesso effettuata o non sono state attuate misure di attenuazione proporzionate, come prescritto al punto 7;

c) il costruttore del veicolo non ha messo in atto misure adeguate e proporzionate per garantire che (se previsti) sul tipo di veicolo siano presenti ambienti dedicati per conservare e far funzionare software, servizi, applicazioni o dati post-vendita;

d) il costruttore del veicolo non ha effettuato, prima dell'omologazione, prove adeguate e sufficienti per verificare l'efficacia delle misure di sicurezza attuate.

5.1.4 L'autorità di omologazione competente per la valutazione deve altresì rifiutarsi di rilasciare l'omologazione per quanto riguarda la cibersicurezza se l'autorità di omologazione stessa o il servizio tecnico non hanno ricevuto dal costruttore del veicolo informazioni sufficienti per valutare la cibersicurezza del tipo di veicolo.

5.2. L'omologazione, l'estensione o il rifiuto dell'omologazione di un tipo di veicolo a norma del presente regolamento devono essere comunicati alle parti dell'accordo del 1958 che applicano il presente regolamento mediante una scheda conforme al modello che figura nell'allegato 2 del presente regolamento.

5.3. Le autorità di omologazione non devono rilasciare omologazioni senza verificare che il costruttore abbia posto in essere disposizioni e procedure soddisfacenti per gestire correttamente gli aspetti della cibersicurezza di cui al presente regolamento.

5.3.1. Oltre ai criteri di cui all'allegato 2 dell'accordo del 1958, l'autorità di omologazione e i suoi servizi tecnici devono garantire di disporre di:

a) personale in possesso di adeguate competenze in materia di cibersicurezza e di conoscenze specifiche in materia di valutazione del rischio nel settore automobilistico ([1]);

b) procedure in atto per la valutazione uniforme in conformità al presente regolamento.

5.3.2. Ciascuna parte contraente che applica il presente regolamento deve notificare e informare, attraverso la propria autorità di omologazione, le altre autorità di omologazione delle parti contraenti che applicano il presente regolamento ONU in merito al metodo e ai criteri utilizzati come base dall'autorità che effettua la notifica per valutare l'adeguatezza delle misure adottate in conformità al presente regolamento, in particolare i punti 5.1, 7.2 e 7.3.

Tali informazioni devono essere condivise a) solo prima che un'omologazione in conformità al presente regolamento sia rilasciata per la prima volta e b) ogni volta che il metodo o i criteri di valutazione sono aggiornati.

Tali informazioni sono condivise ai fini della raccolta e dell'analisi delle migliori pratiche, nonché allo scopo di garantire l'applicazione convergente del presente regolamento da parte di tutte le autorità di omologazione che lo applicano.

5.3.3. Le informazioni di cui al punto 5.3.2 devono essere caricate in lingua inglese nella banca dati protetta "DETA" ([2]), istituita dalla Commissione economica per l'Europa delle Nazioni Unite e accessibile via internet, in tempo utile e non oltre 14 giorni prima che sia rilasciata per la prima volta un'omologazione secondo i metodi e i criteri di valutazione in questione. Le informazioni devono essere sufficienti per comprendere i livelli minimi di prestazione adottati dall'autorità di omologazione per ciascuna prescrizione specifica di cui al punto 5.3.2, nonché i processi e le misure da essa applicati per verificare il rispetto di tali livelli minimi di prestazione ([3]).

5.3.4. Le autorità di omologazione che ricevono le informazioni di cui al punto 5.3.2 possono presentare osservazioni all'autorità di omologazione che effettua la notifica caricandole in DETA entro 14 giorni dal giorno della notifica.

5.3.5. Se l'autorità di omologazione competente per il rilascio non può tenere conto delle osservazioni ricevute in conformità al punto 5.3.4, le autorità di omologazione che hanno inviato osservazioni e l'autorità di omologazione competente per il rilascio devono richiedere ulteriori chiarimenti conformemente alla scheda 6 dell'accordo del 1958. Il pertinente gruppo di lavoro sussidiario ([4]) del Forum mondiale per l'armonizzazione dei regolamenti sui veicoli (WP.29) per il presente regolamento deve concordare un'interpretazione comune dei metodi e dei criteri di valutazione ([5]). Tale interpretazione comune deve essere applicata e tutte le autorità di omologazione devono rilasciare di conseguenza omologazioni a norma del presente regolamento.

([1]) Ad esempio ISO 26262-2018, ISO/PAS 21448, ISO/SAE 21434.
([2]) https://www.unece.org/trans/main/wp29/datasharing.html.
([3]) Nel documento di interpretazione che la task force per la sicurezza informatica e le questioni relative alle trasmissioni senza fili sta elaborando per la settima sessione del GRVA devono essere forniti orientamenti sulle informazioni dettagliate da caricare (ad esempio metodo, criteri, livello di prestazione) e sul formato.
([4]) Il gruppo di lavoro sui veicoli automatizzati/autonomi e connessi (GRVA).
([5]) Tale interpretazione deve essere inclusa nel documento di interpretazione di cui alla nota a piè di pagina del punto 5.3.3.

5.3.6. Ciascuna autorità di omologazione che rilascia un'omologazione a norma del presente regolamento deve notificare l'omologazione rilasciata alle altre autorità di omologazione. L'autorità di omologazione deve caricare l'omologazione in DETA insieme alla documentazione integrativa in lingua inglese entro 14 giorni dalla data di rilascio dell'omologazione ([6]).

5.3.7. Le parti contraenti possono esaminare le omologazioni rilasciate sulla base delle informazioni caricate conformemente al punto 5.3.6. In caso di divergenza di opinioni tra le parti contraenti, la questione deve essere risolta conformemente all'articolo 10 e alla scheda 6 dell'accordo del 1958. Le parti contraenti devono informare inoltre il pertinente gruppo di lavoro sussidiario del Forum mondiale per l'armonizzazione dei regolamenti sui veicoli (WP.29) in merito alle interpretazioni divergenti ai sensi della scheda 6 dell'accordo del 1958. Il gruppo di lavoro competente deve sostenere la risoluzione delle divergenze di opinioni e, ove pertinente, può consultare il WP.29 al riguardo.

5.4. Ai fini del punto 7.2 del presente regolamento, il costruttore deve garantire l'attuazione degli aspetti di cibersicurezza disciplinati dal presente regolamento.

6. Certificato di conformità del sistema di gestione della cibersicurezza

6.1. Le parti contraenti devono incaricare un'autorità di omologazione di effettuare la valutazione del costruttore e di rilasciare un certificato di conformità del CSMS.

6.2. La domanda di certificato di conformità del sistema di gestione della cibersicurezza deve essere presentata dal costruttore del veicolo o da un suo mandatario accreditato.

6.3. La domanda deve essere accompagnata dai documenti indicati nel seguito, in triplice copia, e dalle informazioni seguenti:

6.3.1. documenti che descrivono il sistema di gestione della cibersicurezza;

6.3.2. una dichiarazione firmata utilizzando il modello di cui all'allegato 1, appendice 1.

6.4. Nel contesto della valutazione, il costruttore deve dichiarare, utilizzando il modello di cui all'allegato 1, appendice 1, e dimostrare all'autorità di omologazione o al suo servizio tecnico, di disporre dei processi necessari per soddisfare tutte le prescrizioni in materia di cibersicurezza in conformità al presente regolamento.

6.5. Se gli esiti della valutazione sono soddisfacenti e previo ricevimento di una dichiarazione firmata del costruttore in conformità al modello di cui all'allegato 1, appendice 1, al costruttore deve essere rilasciato il certificato di conformità del CSMS descritto nell'allegato 4 del presente regolamento (in seguito denominato il "certificato di conformità del CSMS").

6.6. L'autorità di omologazione o il suo servizio tecnico devono utilizzare il modello di cui all'allegato 4 del presente regolamento per il certificato di conformità del CSMS.

6.7. Il certificato di conformità del CSMS deve rimanere valido per un massimo di tre anni a decorrere dalla data di rilascio del certificato, a meno che non venga revocato.

6.8. L'autorità di omologazione che ha rilasciato il certificato di conformità del CSMS può verificare in qualsiasi momento che le relative prescrizioni continuino a essere soddisfatte. L'autorità di omologazione deve revocare il certificato di conformità del CSMS se le prescrizioni di cui al presente regolamento non sono più soddisfatte.

([6]) Nel corso della sua settima sessione il GRVA elaborerà ulteriori informazioni sulle prescrizioni minime per il fascicolo di documentazione.

6.9. Il costruttore deve informare l'autorità di omologazione o il suo servizio tecnico di qualsiasi modifica che incida sulla pertinenza del certificato di conformità del CSMS. Dopo aver consultato il costruttore, l'autorità di omologazione o il suo servizio tecnico devono decidere se siano necessari nuovi controlli.

6.10. Il costruttore deve chiedere un nuovo certificato di conformità del CSMS o l'estensione della validità del certificato esistente con un anticipo sufficiente a consentire all'autorità di omologazione di completare la propria valutazione prima della fine del periodo di validità del certificato esistente. Nel caso in cui la valutazione abbia esito positivo, l'autorità di omologazione deve rilasciare un nuovo certificato di conformità del CSMS o prorogare la validità del certificato esistente per un ulteriore periodo di tre anni. L'autorità di omologazione deve verificare che il CSMS continui a soddisfare le prescrizioni del presente regolamento. L'autorità di omologazione deve rilasciare un nuovo certificato nei casi in cui le modifiche portate all'attenzione dell'autorità di omologazione o del suo servizio tecnico abbiano a loro volta ottenuto una valutazione positiva.

6.11. La scadenza o la revoca del certificato di conformità del CSMS del costruttore deve essere considerata, per quanto riguarda i tipi di veicolo per i quali il CSMS in questione era pertinente, come una modifica dell'omologazione, di cui al punto 8, che può comportare la revoca dell'omologazione se le condizioni per il rilascio dell'omologazione non sono più soddisfatte.

7. Specifiche

7.1. Specifiche generali

7.1.1. Le prescrizioni del presente regolamento non devono limitare le disposizioni o le prescrizioni di altri regolamenti ONU.

7.2. Prescrizioni per il sistema di gestione della cibersicurezza

7.2.1. Per la valutazione, l'autorità di omologazione o il suo servizio tecnico devono verificare che il costruttore del veicolo disponga di un sistema di gestione della cibersicurezza e accertarne la conformità al presente regolamento.

7.2.2. Il sistema di gestione della cibersicurezza deve contemplare gli aspetti seguenti:

7.2.2.1. il costruttore del veicolo deve dimostrare a un'autorità di omologazione o a un servizio tecnico che il suo sistema di gestione della cibersicurezza si applica alle fasi seguenti:

a) fase di sviluppo;

b) fase di produzione;

c) fase di post-produzione;

7.2.2.2. il costruttore del veicolo deve dimostrare che i processi utilizzati nell'ambito del suo sistema di gestione della cibersicurezza garantiscono che la sicurezza sia stata adeguatamente presa in considerazione, anche in relazione ai rischi e alle misure di attenuazione elencati nell'allegato 5. Tali processi devono includere:

a) i processi utilizzati all'interno dell'organizzazione del costruttore per gestire la cibersicurezza;

b) i processi utilizzati per l'identificazione dei rischi per i tipi di veicolo. Nell'ambito di tali processi devono essere prese in considerazione le minacce di cui all'allegato 5, parte A, e altre minacce pertinenti;

c) i processi utilizzati per la valutazione, la categorizzazione e il trattamento dei rischi individuati;

d) i processi in atto per verificare che i rischi individuati siano gestiti in modo adeguato;

e) i processi utilizzati per testare la cibersicurezza di un tipo di veicolo;

f) i processi utilizzati per garantire che la valutazione del rischio sia mantenuta aggiornata;

g) i processi utilizzati per monitorare, individuare e rispondere agli attacchi informatici, alle minacce informatiche e alle vulnerabilità dei tipi di veicolo e i processi utilizzati per valutare se le misure di cibersicurezza attuate siano ancora efficaci alla luce delle nuove minacce informatiche e vulnerabilità individuate;

h) i processi utilizzati per fornire dati pertinenti a sostegno dell'analisi di attacchi informatici tentati o riusciti;

7.2.2.3. il costruttore del veicolo deve dimostrare che i processi utilizzati nel suo sistema di gestione della cibersicurezza garantiranno che, sulla base della categorizzazione di cui al punto 7.2.2.2, lettere c) e g), le minacce informatiche e le vulnerabilità che richiedono una risposta da parte del costruttore del veicolo siano attenuate entro un lasso di tempo ragionevole;

7.2.2.4. il costruttore del veicolo deve dimostrare che i processi utilizzati nel suo sistema di gestione della cibersicurezza garantiscono che il monitoraggio di cui al punto 7.2.2.2, lettera g), sia continuo. Esso deve:

a) includere i veicoli nel monitoraggio dopo la prima immatricolazione;

b) includere la capacità di analizzare e rilevare minacce informatiche, vulnerabilità e attacchi informatici attraverso i dati e i log dei veicoli. Tale capacità deve rispettare il punto 1.3 e i diritti alla privacy dei proprietari di automobili o dei conducenti, in particolare per quanto riguarda il consenso;

7.2.2.5. il costruttore del veicolo deve essere tenuto a dimostrare in che modo il suo sistema di gestione della cibersicurezza gestirà le eventuali dipendenze con fornitori, fornitori di servizi o sotto-organizzazioni del costruttore per quanto riguarda le prescrizioni di cui al punto 7.2.2.2.

7.3. Prescrizioni per i tipi di veicolo

7.3.1. Il costruttore deve essere in possesso di un certificato di conformità valido per il sistema di gestione della cibersicurezza relativo al tipo di veicolo da omologare. Tuttavia, per le omologazioni dei veicoli delle categorie M, N e O rilasciate per la prima volta prima del 1º luglio 2024, e per le omologazioni dei veicoli della categoria L rilasciate per la prima volta prima del 1º luglio 2029, e per ciascuna estensione delle stesse, se il costruttore del veicolo è in grado di dimostrare che non è stato possibile sviluppare il tipo di veicolo in maniera conforme al CSMS, il costruttore del veicolo deve dimostrare che la cibersicurezza è stata adeguatamente presa in considerazione durante la fase di sviluppo del tipo di veicolo in questione.

7.3.2. Il costruttore del veicolo deve individuare e gestire, per il tipo di veicolo da omologare, i rischi connessi ai fornitori.

7.3.3. Il costruttore del veicolo deve individuare gli elementi critici del tipo di veicolo ed effettuare un'esauriente valutazione del rischio per il tipo di veicolo e deve trattare/gestire adeguatamente i rischi individuati. La valutazione del rischio deve prendere in considerazione i singoli elementi del tipo di veicolo e le loro interazioni. La valutazione del rischio deve inoltre prendere in considerazione le interazioni con eventuali sistemi esterni. Nel valutare i rischi, il costruttore del veicolo deve tenere conto dei rischi connessi a tutte le minacce di cui all'allegato 5, parte A, nonché di qualsiasi altro rischio pertinente.

7.3.4. Il costruttore del veicolo deve proteggere il tipo di veicolo dai rischi individuati nella sua valutazione del rischio. Devono essere attuate misure di attenuazione proporzionate per proteggere il tipo di veicolo. Le misure attuate devono includere tutte le misure di attenuazione di cui all'allegato 5, parti B e C, che sono pertinenti per i rischi individuati. Tuttavia, se una delle misure di attenuazione di cui all'allegato 5, parte B o C, non è pertinente o non è sufficiente per il rischio individuato, il costruttore del veicolo deve garantire che venga attuata un'altra misura di attenuazione adeguata.

In particolare, per le omologazioni dei veicoli delle categorie M, N e O rilasciate per la prima volta prima del 1° luglio 2024, e per le omologazioni dei veicoli della categoria L rilasciate per la prima volta prima del 1° luglio 2029, e per ciascuna estensione delle stesse, il costruttore del veicolo deve garantire che venga attuata un'altra misura di attenuazione adeguata se una delle misure di attenuazione di cui all'allegato 5, parte B o C, non è tecnicamente fattibile. La rispettiva valutazione dell'applicabilità tecnica deve essere fornita dal costruttore all'autorità di omologazione.

7.3.5. Il costruttore del veicolo deve mettere in atto misure adeguate e proporzionate per garantire che (se previsti) sul tipo di veicolo siano presenti ambienti dedicati per conservare e far funzionare di software, servizi, applicazioni o dati post-vendita.

7.3.6. Il costruttore del veicolo deve effettuare, prima dell'omologazione, prove adeguate e sufficienti per verificare l'efficacia delle misure di sicurezza attuate.

7.3.7. Il costruttore del veicolo deve attuare misure per il tipo di veicolo al fine di:

a) rilevare e prevenire gli attacchi informatici nei confronti dei veicoli appartenenti al tipo di veicolo in questione;

b) potenziare la sua capacità di monitoraggio per quanto riguarda l'individuazione di minacce, vulnerabilità e attacchi informatici pertinenti al tipo di veicolo;

c) disporre di capacità di trattamento dei dati che consentano di analizzare gli attacchi informatici tentati o riusciti.

7.3.8. I moduli crittografici utilizzati ai fini del presente regolamento devono essere in linea con le norme concordate. Se i moduli crittografici utilizzati non sono in linea con le norme concordate, il costruttore del veicolo ne deve giustificare l'uso.

7.4. Disposizioni in materia di comunicazione

7.4.1. Il costruttore del veicolo deve riferire almeno una volta all'anno, o più frequentemente se del caso, all'autorità di omologazione o al servizio tecnico in merito ai risultati delle sue attività di monitoraggio, quali definite al punto 7.2.2.2, lettera g), comprese le informazioni pertinenti sui nuovi attacchi informatici. Il costruttore del veicolo deve inoltre comunicare e confermare all'autorità di omologazione o al servizio tecnico che le misure di attenuazione in materia di cibersicurezza attuate in relazione ai suoi tipi di veicolo sono ancora efficaci e le eventuali azioni supplementari intraprese.

7.4.2 L'autorità di omologazione o il servizio tecnico devono verificare le informazioni fornite e, se necessario, esigere che il costruttore del veicolo ponga rimedio alle eventuali inefficienze rilevate.

Se la comunicazione o la risposta non è sufficiente, l'autorità di omologazione può decidere di revocare il certificato di conformità del CSMS in conformità al punto 6.8.

8. Modifica del tipo di veicolo ed estensione dell'omologazione

8.1. Ogni modifica del tipo di veicolo che incida sulle prestazioni tecniche per quanto riguarda la cibersicurezza e/o sulla documentazione richiesta dal presente regolamento deve essere notificata all'autorità di omologazione che ha omologato il tipo di veicolo. Tale autorità può quindi:

8.1.1. ritenere che le modifiche apportate siano ancora conformi alle prescrizioni e alla documentazione dell'omologazione esistente; oppure

8.1.2. procedere alla necessaria valutazione complementare a norma del punto 5 e richiedere, se del caso, un ulteriore verbale di prova al servizio tecnico incaricato di eseguire le prove.

8.1.3. La conferma, l'estensione o il rifiuto dell'omologazione, con indicazione delle modifiche apportate, devono essere comunicati mediante una scheda di notifica conforme al modello figurante nell'allegato 2 del presente regolamento. L'autorità di omologazione che rilascia l'estensione dell'omologazione deve assegnare un numero di serie all'estensione e informare le altre parti dell'accordo del 1958 che applicano il presente regolamento mediante una scheda di notifica conforme al modello figurante nell'allegato 2 del presente regolamento.

9. Conformità della produzione

9.1. Le procedure per il controllo della conformità della produzione devono essere conformi a quelle indicate nell'allegato 1 dell'accordo del 1958 (E/ECE/TRANS/505/Rev.3), nonché alle prescrizioni seguenti:

9.1.1. il titolare dell'omologazione deve garantire che i risultati delle prove di conformità della produzione siano registrati e che i documenti allegati restino a disposizione per un periodo di tempo concordato con l'autorità di omologazione o con il suo servizio tecnico. Tale periodo non deve essere superiore a 10 anni a partire dalla cessazione definitiva della produzione;

9.1.2. l'autorità che ha rilasciato l'omologazione ha facoltà di verificare in qualsiasi momento i metodi di controllo della conformità applicati in ogni stabilimento di produzione. Tali verifiche devono avere di norma cadenza triennale.

10. Sanzioni in caso di non conformità della produzione

10.1. L'omologazione di un tipo di veicolo rilasciata a norma del presente regolamento può essere revocata se cessano di essere soddisfatte le prescrizioni di cui al presente regolamento o se i veicoli campione non sono conformi alle prescrizioni del presente regolamento.

10.2. Se un'autorità di omologazione revoca un'omologazione da essa in precedenza rilasciata, deve informare immediatamente le parti contraenti che applicano il presente regolamento mediante una scheda di notifica conforme al modello figurante nell'allegato 2 del presente regolamento.

11. Cessazione definitiva della produzione

11.1. Se il titolare di un'omologazione cessa definitivamente la produzione di un tipo di veicolo omologato a norma del presente regolamento, deve informarne l'autorità che ha rilasciato l'omologazione. Appena ricevuta la relativa notifica, tale autorità deve informare le altre parti dell'accordo che applicano il presente regolamento inviando una copia della scheda di omologazione recante in calce, a chiare lettere, l'annotazione firmata e datata "PRODUZIONE CESSATA".

12. Nomi e indirizzi dei servizi tecnici responsabili delle prove di omologazione e delle autorità di omologazione

12.1. Le parti dell'accordo che applicano il presente regolamento devono comunicare al segretariato delle Nazioni Unite i nomi e gli indirizzi dei servizi tecnici incaricati di eseguire le prove di omologazione e delle autorità che rilasciano le omologazioni e alle quali devono essere inviate le schede attestanti il rilascio, l'estensione, il rifiuto o la revoca di omologazioni rilasciate in altri paesi.

ALLEGATO 1

Scheda informativa

Le seguenti informazioni devono essere fornite, ove pertinente, in triplice copia e devono contenere un indice. Gli eventuali disegni devono essere forniti in scala adeguata e con sufficienti dettagli, in formato A4 o in fogli piegati in tale formato. Le eventuali fotografie devono mostrare sufficienti dettagli.

1. Marchio (denominazione commerciale del costruttore):.....

2. Tipo e descrizione/i commerciale/i generale/i:.....

3. Mezzi di identificazione del tipo, se marcati sul veicolo:.....

4. Posizione di tale indicazione: .....

5. Categoria/e del veicolo:.....

6. Nome e indirizzo del costruttore/mandatario del costruttore:.....

7. Nome/i e indirizzo/i dello/degli stabilimento/i di montaggio: .....

8. Fotografie e/o disegni di un veicolo rappresentativo: .....

9. Cibersicurezza

9.1. Caratteristiche costruttive generali del tipo di veicolo, ivi compresi:

a) i sistemi del veicolo che sono pertinenti alla cibersicurezza del tipo di veicolo;

b) i componenti di tali sistemi che sono pertinenti alla cibersicurezza;

c) le interazioni di tali sistemi con altri sistemi all'interno del tipo di veicolo e con le interfacce esterne.

9.2. Rappresentazione schematica del tipo di veicolo

9.3. Numero del certificato di conformità del CSMS:.....

9.4. Documenti per il tipo di veicolo da omologare che descrivono l'esito della valutazione del rischio e i rischi individuati: .....

9.5. Documenti per il tipo di veicolo da omologare che descrivono le misure di attenuazione applicate ai sistemi elencati o al tipo di veicolo e il modo in cui affrontano i rischi dichiarati: .....

9.6. Documenti per il tipo di veicolo da omologare che descrivono la protezione degli ambienti dedicati per software, servizi, applicazioni o dati post-vendita:.....

9.7. Documenti per il tipo di veicolo da omologare che descrivono le prove utilizzate per verificare la cibersicurezza del tipo di veicolo e dei suoi sistemi e l'esito di tali prove:.....

9.8. Descrizione delle modalità con cui si è tenuto conto della catena di approvvigionamento per quanto riguarda la cibersicurezza:.....

Allegato 1 - Appendice 1

Modello di dichiarazione di conformità del CSMS del costruttore

Dichiarazione del costruttore attestante la conformità alle prescrizioni per il sistema di gestione della cibersicurezza

Nome del costruttore: ……

Indirizzo del costruttore: ……

…… (*nome del costruttore*)

attesta che i processi necessari per conformare il sistema di gestione della cibersicurezza alle prescrizioni di cui al punto 7.2 del regolamento UNECE n. 155 sono stati predisposti e saranno mantenuti.

Fatto a: ……(*luogo*)

Data:……

Nome del firmatario: ……

Funzione del firmatario:……

(Timbro e firma del mandatario del costruttore)

ALLEGATO 2

Notifica

(formato massimo: A4 (210 × 297 mm))



Emessa da: Nome dell'amministrazione:
……
……
……

Relativa a (2): rilascio dell'omologazione
estensione dell'omologazione
revoca dell'omologazione con effetto dal gg/mm/aaaa
rifiuto dell'omologazione
cessazione definitiva della produzione

di un tipo di veicolo a norma del regolamento UNECE n. 155

Omologazione n.:……

Estensione n.:……

Motivo dell'estensione:……

1. Marchio (denominazione commerciale del costruttore):……

2. Tipo e descrizione commerciale generale:……

3. Mezzi di identificazione del tipo, se marcati sul veicolo:……

3.1. Posizione di tale indicazione:……

4. Categoria/e del veicolo:……

5. Nome e indirizzo del costruttore/mandatario del costruttore:……

6. Nomi e indirizzi degli stabilimenti di produzione:……

7. Numero del certificato di conformità del sistema di gestione della cibersicurezza:……

8. Servizio tecnico incaricato di eseguire le prove:……

9. Data del verbale di prova:……

10. Numero del verbale di prova:……

11. Osservazioni: (se del caso).……

12. Luogo:……

(1) Numero distintivo del paese che ha rilasciato/esteso/rifiutato/revocato l'omologazione (cfr. disposizioni sull'omologazione contenute nel regolamento).
(2) Cancellare quanto non pertinente.

13. Data:……

14. Firma:……

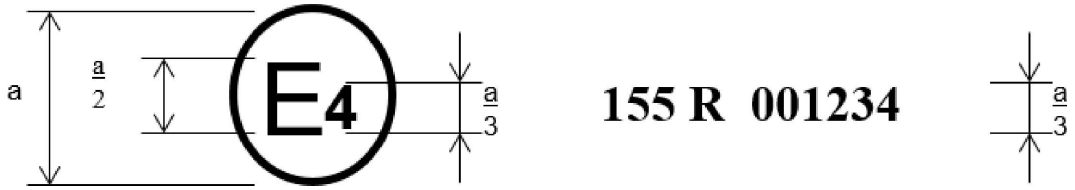
15. Si allega l'indice del fascicolo informativo depositato presso l'autorità di omologazione, del quale si può richiedere copia:

ALLEGATO 3

Esempio di marchio di omologazione

MODELLO A

(cfr. punto 4.2 del presente regolamento)



a = 8 mm min.

Il marchio di omologazione sopra raffigurato, apposto su un veicolo, indica che il tipo di veicolo stradale in questione è stato omologato nei Paesi Bassi (E4), a norma del regolamento n. 155 e con il numero di omologazione 001234. Le prime due cifre del numero di omologazione indicano che l'omologazione è stata rilasciata conformemente alle prescrizioni del regolamento nella sua versione originale (00).

ALLEGATO 4

MODELLO DI CERTIFICATO DI CONFORMITÀ DEL CSMS

Certificato di conformità del sistema di gestione della cibersicurezza

al regolamento UNECE n. 155

Numero del certificato [*numero di riferimento*]

[……. *autorità di omologazione*]

certifica che

Costruttore:……

Indirizzo del costruttore: ……

è conforme alle disposizioni del punto 7.2 del regolamento n. 155

Sono stati effettuati controlli su:……

da (nome e indirizzo dell'autorità di omologazione o del servizio tecnico): ……

Numero del verbale:……

Il certificato è valido fino a […… *data*]

Fatto a [……*luogo*]

Il […… *data*]

[…… *firma*]

Allegati: descrizione del sistema di gestione della cibersicurezza da parte del costruttore.

ALLEGATO 5

Elenco delle minacce e delle misure di attenuazione corrispondenti

1. Il presente allegato si compone di tre parti. La parte A descrive la base di riferimento per le minacce, le vulnerabilità e i metodi di attacco. La parte B descrive le misure di attenuazione delle minacce destinate ai tipi di veicolo. La parte C descrive le misure di attenuazione delle minacce destinate ad ambiti esterni ai veicoli, ad esempio il back-end informatico.

2. Le parti A, B e C devono essere prese in considerazione ai fini della valutazione del rischio e delle misure di attenuazione che devono essere attuate dai costruttori di veicoli.

3. Alle vulnerabilità di alto livello e agli esempi corrispondenti è stato assegnato un indice nella parte A. La stessa indicizzazione è stata riportata nelle tabelle delle parti B e C per collegare ciascun attacco/vulnerabilità a un elenco di misure di attenuazione corrispondenti.

4. L'analisi delle minacce deve tenere conto anche dei possibili impatti degli attacchi. Questi possono contribuire a determinare la gravità di un rischio e a individuare ulteriori rischi. I possibili impatti degli attacchi possono comprendere:

   a) compromissione del funzionamento sicuro del veicolo;

   b) cessazione dell'operatività di funzioni del veicolo;

   c) modifiche del software, alterazioni delle prestazioni;

   d) alterazioni del software, ma senza conseguenze sul funzionamento;

   e) violazione dell'integrità dei dati;

   f) violazione della riservatezza dei dati;

   g) perdita di disponibilità dei dati;

   h) altro, compresi atti criminosi.

PARTE A.

Vulnerabilità o metodi di attacco connessi alle minacce

Le descrizioni ad alto livello delle minacce e delle relative vulnerabilità o dei relativi metodi di attacco sono riportate nella tabella A1.

Tabella A1

Elenco delle vulnerabilità o dei metodi di attacco connessi alle minacce

Descrizioni delle vulnerabilità/minacce di livello superiore e di livello inferiore			Esempio di vulnerabilità o di metodo di attacco	
4.3.1. Minacce relative ai server di back-end connessi ai veicoli in circolazione	1	Server di back-end utilizzati come mezzo per attaccare un veicolo o estrarre dati	1.1	Abuso di privilegi da parte del personale (attacco dall'interno)
			1.2	Accesso internet non autorizzato al server (attivato ad esempio tramite backdoor, vulnerabilità del software di sistema non corrette tramite patch, attacchi SQL o altri mezzi)
			1.3	Accesso fisico non autorizzato al server (effettuato ad esempio mediante chiavette USB o altri supporti che si collegano al server)
	2	Perturbazione dei servizi del server di back-end che incide sul funzionamento di un veicolo	2.1	L'attacco al server di back-end ne blocca il funzionamento, ad esempio impedendogli di interagire con i veicoli e di fornire i servizi su cui questi ultimi fanno affidamento

Descrizioni delle vulnerabilità/minacce di livello superiore e di livello inferiore			Esempio di vulnerabilità o di metodo di attacco	
	3	Perdita o compromissione dei dati relativi ai veicoli conservati su server di back-end ("violazione dei dati")	3.1	Abuso di privilegi da parte del personale (attacco dall'interno)
			3.2	Perdita di informazioni nel cloud. I dati sensibili conservati presso fornitori terzi di servizi cloud possono andare perduti a causa di attacchi o incidenti
			3.3	Accesso internet non autorizzato al server (attivato ad esempio tramite backdoor, vulnerabilità del software di sistema non corrette tramite patch, attacchi SQL o altri mezzi)
			3.4	Accesso fisico non autorizzato al server (effettuato ad esempio mediante chiavette USB o altri supporti che si collegano al server)
			3.5	Violazione delle informazioni dovuta alla condivisione non intenzionale di dati (ad esempio errori amministrativi)
4.3.2 Minacce ai veicoli per quanto riguarda i loro canali di comunica-zione	4	Spoofing di messaggi o dati ricevuti dal veicolo	4.1	Spoofing dei messaggi (ad esempio messaggi di consapevolezza cooperativa V2X o di coordinamento delle manovre, messaggi GNSS ecc.) mediante impersonificazione
			4.2	Attacco Sybil (al fine di simulare la presenza di altri veicoli per fingere che ve ne siano molti sulla strada)
	5	Canali di comunicazione utilizzati per effettuare manipolazioni, cancellazioni o altre modifiche non autorizzate del codice/dei dati detenuti dal veicolo	5.1	I canali di comunicazione consentono l'iniezione di codice; ad esempio un codice binario manomesso potrebbe essere iniettato nel flusso di comunicazione
			5.2	I canali di comunicazione consentono la manipolazione del codice/dei dati detenuti dal veicolo
			5.3	I canali di comunicazione consentono la sovrascrittura del codice/dei dati detenuti dal veicolo
			5.4	I canali di comunicazione consentono la cancellazione del codice/dei dati detenuti dal veicolo
			5.5	I canali di comunicazione consentono l'introduzione di codice/dati nel veicolo (codice per la scrittura di dati)
	6	I canali di comunicazione consentono di accettare messaggi non attendibili/ inaffidabili o sono vulnerabili agli attacchi replay/di dirottamento di sessione	6.1	Accettazione di informazioni da una fonte inaffidabile o non attendibile
			6.2	Attacco "man in the middle"/dirottamento di sessione
			6.3	Attacco replay, ad esempio un attacco contro un gateway di comunicazione che consente all'aggressore di installare una versione precedente del software di una centralina elettronica o del firmware del gateway
	7	Le informazioni possono essere facilmente divulgate, ad esempio intercettando le comunicazioni o consentendo l'accesso non autorizzato a file o cartelle sensibili	7.1	Intercettazione di informazioni/radiazioni interferenti/monitoraggio delle comunicazioni
			7.2	Ottenimento di un accesso non autorizzato a file o dati

Descrizioni delle vulnerabilità/minacce di livello superiore e di livello inferiore			Esempio di vulnerabilità o di metodo di attacco	
	8	Attacchi "Denial of Service" attraverso canali di comunicazione per perturbare le funzioni del veicolo	8.1	Invio di una grande quantità di dati spazzatura al sistema informatico del veicolo in modo che questo non sia in grado di fornire servizi in modo normale
			8.2	Attacco "black hole", in cui l'aggressore è in grado di bloccare i messaggi tra i veicoli al fine di perturbare la comunicazione tra gli stessi
	9	Un utente senza privilegi è in grado di ottenere un accesso privilegiato ai sistemi dei veicoli	9.1	Un utente senza privilegi è in grado di ottenere un accesso privilegiato, ad esempio un accesso root
	10	I virus incorporati nei mezzi di comunicazione sono in grado di infettare i sistemi dei veicoli	10.1	Il virus incorporato nei mezzi di comunicazione infetta i sistemi dei veicoli
	11	I messaggi ricevuti dal veicolo (ad esempio X2V o messaggi diagnostici), o trasmessi al suo interno, contengono contenuti malevoli	11.1	Messaggi (ad esempio CAN) interni malevoli
			11.2	Messaggi V2X malevoli, ad esempio messaggi da infrastruttura a veicolo o veicolo-veicolo (ad esempio CAM, DENM)
			11.3	Messaggi diagnostici malevoli
			11.4	Messaggi proprietari malevoli (ad esempio quelli normalmente inviati dall'OEM o dal fornitore di componenti/sistemi/funzioni)
4.3.3 Minacce ai veicoli per quanto riguarda le loro procedure di aggiornamento	12	Uso improprio o compromissione delle procedure di aggiornamento	12.1	Compromissione delle procedure di aggiornamento OTA dei software, compresa la creazione di un falso firmware o programma di aggiornamento del sistema
			12.2	Compromissione delle procedure di aggiornamento locale/fisico del software, compresa la creazione di un falso firmware o programma di aggiornamento del sistema
			12.3	Il software è manipolato prima del processo di aggiornamento (ed è quindi corrotto), sebbene il processo di aggiornamento sia intatto
			12.4	Compromissione delle chiavi crittografiche del fornitore di software per consentire un aggiornamento non valido
	13	Possibilità di negare gli aggiornamenti legittimi	13.1	Attacco "Denial of Service" contro un server o una rete di aggiornamento per impedire l'installazione di aggiornamenti critici del software e/o lo sblocco di funzioni specifiche del cliente
4.3.4. Minacce ai veicoli per quanto riguarda le azioni umane non intenzionali che facilitano un attacco informatico	15	I soggetti autorizzati sono in grado di compiere azioni che potrebbero facilitare inconsapevolmente un attacco informatico	15.1	Una vittima inconsapevole (ad esempio un proprietario, un operatore o un addetto alla manutenzione) è indotta a compiere un'azione che comporta il caricamento involontario di malware o che consente un attacco
			15.2	Le procedure di sicurezza definite non sono rispettate

Descrizioni delle vulnerabilità/minacce di livello superiore e di livello inferiore			Esempio di vulnerabilità o di metodo di attacco	
4.3.5. Minacce ai veicoli per quanto riguarda la connettività e i collegamenti esterni	16	La manipolazione della connettività delle funzioni del veicolo consente un attacco informatico; sono inclusi la telematica, i sistemi che consentono le operazioni a distanza e sistemi che utilizzano comunicazioni senza fili a corto raggio	16.1	Manipolazione di funzioni progettate per comandare i sistemi a distanza, come la chiave telecomando, l'immobilizzatore e la colonnina di carica
			16.2	Manipolazione della telematica dei veicoli (ad esempio manipolazione della misurazione della temperatura di merci sensibili, sblocco a distanza dei portelloni di carico)
			16.3	Interferenza con sistemi o sensori senza fili a corto raggio
	17	Software di terzi ospitati sul veicolo, ad esempio applicazioni di intrattenimento, utilizzati come mezzo per attaccare i sistemi dei veicoli	17.1	Applicazioni corrotte o con scarsa sicurezza del software, utilizzate come metodo per attaccare i sistemi dei veicoli
	18	Dispositivi collegati a interfacce esterne, ad esempio porte USB, porte OBD, utilizzati come mezzo per attaccare i sistemi del veicolo	18.1	Interfacce esterne quali USB o altre porte utilizzate come punto di attacco, ad esempio mediante iniezione di codice
			18.2	Supporti infettati da un virus collegato a un sistema di un veicolo
			18.3	Accesso diagnostico (ad esempio dongle nella porta OBD) utilizzato per facilitare un attacco, ad esempio per manipolare i parametri del veicolo (direttamente o indirettamente)
4.3.6. Minacce al codice/ai dati del veicolo	19	Estrazione di codice/di dati del veicolo	19.1	Estrazione di software proprietario o protetto da diritto d'autore dai sistemi dei veicoli (pirateria di prodotti)
			19.2	Accesso non autorizzato a informazioni private del proprietario, quali l'identità personale, le informazioni sui conti di pagamento, le informazioni sulla rubrica degli indirizzi, le informazioni relative all'ubicazione, l'ID elettronico del veicolo ecc.
			19.3	Estrazione di chiavi crittografiche
	20	Manipolazione del codice/dei dati del veicolo	20.1	Modifiche illegali/non autorizzate all'ID elettronico del veicolo
			20.2	Frode d'identità, ad esempio se un utente vuole mostrare un'altra identità quando comunica con sistemi di pedaggio o con il back-end del costruttore
			20.3	Azioni volte a eludere i sistemi di monitoraggio (ad esempio hackeraggio/manomissione/blocco di messaggi quali i dati ODR Tracker o il numero di esecuzioni)
			20.4	Manipolazione dei dati per falsificare i dati di guida del veicolo (ad esempio chilometraggio, velocità di guida, direzioni di marcia ecc.)
			20.5	Modifiche non autorizzate ai dati diagnostici del sistema
	21	Cancellazione di codice/di dati	21.1	Cancellazione/manipolazione non autorizzata dei log degli eventi di sistema
	22	Introduzione di malware	22.2	Introduzione di software maligni o attività di software maligni

Descrizioni delle vulnerabilità/minacce di livello superiore e di livello inferiore			Esempio di vulnerabilità o di metodo di attacco	
	23	Introduzione di un nuovo software o sovrascrittura di un software esistente	23.1	Creazione di un falso software del sistema di controllo o del sistema informatico del veicolo
	24	Perturbazione di sistemi o operazioni	24.1	Attacco "Denial of Service" che può essere ad esempio innescato sulla rete interna inondando un bus CAN o provocando guasti a una centralina elettronica mediante l'invio di una grande quantità di messaggi
	25	Manipolazione dei parametri del veicolo	25.1	Accesso non autorizzato al fine di falsificare i parametri di configurazione delle funzioni chiave del veicolo, quali i dati dei freni, la soglia di attivazione dell'airbag ecc.
			25.2	Accesso non autorizzato al fine di falsificare i parametri di carica, quali tensione di carica, potenza di carica, temperatura della batteria ecc.
4.3.7. Potenziali vulnerabilità che potrebbero essere sfruttate se non sufficiente-mente protette o rinforzate	26	Le tecnologie crittografiche possono essere compromesse o sono applicate in misura insufficiente	26.1	L'uso di chiavi crittografiche brevi con un lungo periodo di validità consente agli aggressori di violare la cifratura
			26.2	Uso insufficiente di algoritmi crittografici per proteggere i sistemi sensibili
			26.3	Utilizzo di algoritmi crittografici già obsoleti o che lo saranno presto
	27	Parti o forniture potrebbero essere compromesse per consentire attacchi nei confronti dei veicoli	27.1	Hardware o software progettati per consentire un attacco o che non soddisfano i criteri di progettazione per fermare un attacco
	28	Lo sviluppo di software o hardware lascia spazio a vulnerabilità	28.1	Bug del software. La presenza di bug del software può costituire una base per potenziali vulnerabilità sfruttabili. Ciò vale in particolare se il software non è stato testato per verificare l'assenza di codice errato/bug noti e ridurre il rischio di presenza di codice errato/bug sconosciuti
			28.2	L'utilizzo di residui dello sviluppo (ad esempio porte di debug, porte JTAG, microprocessori, certificati di sviluppo, password programmatore ecc.) può consentire l'accesso alle centraline elettroniche o permettere agli aggressori di ottenere privilegi più elevati
	29	La progettazione della rete introduce vulnerabilità	29.1	Porte internet superflue lasciate aperte, che forniscono accesso ai sistemi di rete
			29.2	Elusione della separazione di rete per ottenere il controllo. Un esempio specifico è l'uso di gateway non protetti o di punti di accesso (come i gateway camion-rimorchio) per aggirare le protezioni e ottenere accesso ad altri segmenti di rete al fine di compiere atti malevoli, come l'invio di messaggi arbitrari sul bus CAN
	31	Può verificarsi un trasferimento non intenzionale di dati	31.1	Violazione delle informazioni. I dati personali possono essere sottratti quando l'automobile cambia utente (ad esempio quando viene venduta o utilizzata come veicolo a noleggio con nuovi noleggiatori)

Descrizioni delle vulnerabilità/minacce di livello superiore e di livello inferiore			Esempio di vulnerabilità o di metodo di attacco	
	32	La manipolazione fisica dei sistemi può consentire un attacco	32.1	Manipolazione dell'hardware elettronico, ad esempio se un hardware elettronico non autorizzato è aggiunto a un veicolo per consentire un attacco "man in the middle" Sostituzione dell'hardware elettronico autorizzato (ad esempio sensori) con hardware elettronico non autorizzato Manipolazione delle informazioni raccolte da un sensore (ad esempio mediante l'utilizzo di un magnete per manomettere il sensore ad effetto Hall collegato al cambio)

PARTE B.

Misure di attenuazione delle minacce previste per i veicoli

1. Misure di attenuazione per i "canali di comunicazione dei veicoli"

Le misure di attenuazione delle minacce per quanto riguarda i "canali di comunicazione dei veicoli" sono elencate nella tabella B1.

Tabella B1

Misure di attenuazione delle minacce per quanto riguarda i "canali di comunicazione dei veicoli"

Riferimento tabella A1	Minacce relative ai "canali di comunicazione dei veicoli"	Rif.	Misura di attenuazione
4.1	Spoofing dei messaggi (ad esempio messaggi di consapevolezza cooperativa V2X o di coordinamento delle manovre, messaggi GNSS ecc.) mediante impersonificazione	M10	Il veicolo deve verificare l'autenticità e l'integrità dei messaggi ricevuti
4.2	Attacco Sybil (al fine di simulare la presenza di altri veicoli per fingere che ve ne siano molti sulla strada)	M11	Devono essere effettuati controlli di sicurezza per la conservazione delle chiavi crittografiche (ad esempio utilizzo di moduli di sicurezza hardware)
5.1	I canali di comunicazione consentono l'iniezione di codice all'interno del codice/dei dati detenuti dal veicolo; ad esempio un codice binario manomesso potrebbe essere iniettato nel flusso di comunicazione	M10 M6	Il veicolo deve verificare l'autenticità e l'integrità dei messaggi ricevuti I sistemi devono integrare la sicurezza fin dalla progettazione per ridurre al minimo i rischi
5.2	I canali di comunicazione consentono la manipolazione del codice/dei dati detenuti dal veicolo	M7	Per proteggere il codice/i dati del sistema devono essere applicate tecniche e soluzioni per il controllo degli accessi
5.3	I canali di comunicazione consentono la sovrascrittura del codice/dei dati detenuti dal veicolo		
5.4 21.1	I canali di comunicazione consentono la cancellazione del codice/dei dati detenuti dal veicolo		
5.5	I canali di comunicazione consentono l'introduzione di codice/dati nel veicolo (codice per la scrittura di dati)		

Riferimento tabella A1	Minacce relative ai "canali di comunicazione dei veicoli"	Rif.	Misura di attenuazione
6.1	Accettazione di informazioni da una fonte inaffidabile o non attendibile	M10	Il veicolo deve verificare l'autenticità e l'integrità dei messaggi ricevuti
6.2	Attacco "man in the middle"/ dirottamento di sessione	M10	Il veicolo deve verificare l'autenticità e l'integrità dei messaggi ricevuti
6.3	Attacco replay, ad esempio un attacco contro un gateway di comunicazione che consente all'aggressore di installare una versione precedente del software di una centralina elettronica o del firmware del gateway		
7.1	Intercettazione di informazioni/ radiazioni interferenti/monitoraggio delle comunicazioni	M12	I dati riservati trasmessi al veicolo o dal veicolo devono essere protetti
7.2	Ottenimento di un accesso non autorizzato a file o dati	M8	Attraverso la progettazione del sistema e il controllo degli accessi il personale non autorizzato non dovrebbe poter accedere ai dati personali o critici del sistema. Esempi di controlli di sicurezza sono reperibili in OWASP
8.1	Invio di una grande quantità di dati spazzatura al sistema informatico del veicolo in modo che questo non sia in grado di fornire servizi in modo normale	M13	Devono essere adottate misure per individuare e rimediare a un attacco "Denial of Service"
8.2	Attacco "black hole", perturbazione della comunicazione tra veicoli attraverso il blocco del trasferimento di messaggi ad altri veicoli	M13	Devono essere adottate misure per individuare e rimediare a un attacco "Denial of Service"
9.1	Un utente senza privilegi è in grado di ottenere un accesso privilegiato, ad esempio un accesso root	M9	Devono essere adottate misure per prevenire e individuare l'accesso non autorizzato
10.1	Il virus incorporato nei mezzi di comunicazione infetta i sistemi dei veicoli	M14	Dovrebbero essere prese in considerazione misure volte a proteggere i sistemi da virus/malware incorporati
11.1	Messaggi (ad esempio CAN) interni malevoli	M15	Dovrebbero essere prese in considerazione misure volte a individuare l'attività o i messaggi interni malevoli
11.2	Messaggi V2X malevoli, ad esempio messaggi da infrastruttura a veicolo o veicolo-veicolo (ad esempio CAM, DENM)	M10	Il veicolo deve verificare l'autenticità e l'integrità dei messaggi ricevuti
11.3	Messaggi diagnostici malevoli		
11.4	Messaggi proprietari malevoli (ad esempio quelli normalmente inviati dall'OEM o dal fornitore di componenti/ sistemi/funzioni)		

2. Misure di attenuazione per il ”processo di aggiornamento”

Le misure di attenuazione delle minacce per quanto riguarda il ”processo di aggiornamento” sono elencate nella tabella B2.

Tabella B2

Misure di attenuazione delle minacce per quanto riguarda il ”processo di aggiornamento”

Riferimento tabella A1	Minacce relative al ”processo di aggiornamento”	Rif.	Misura di attenuazione
12.1	Compromissione delle procedure di aggiornamento OTA dei software, compresa la creazione di un falso firmware o programma di aggiornamento del sistema	M16	Devono essere adottate procedure di aggiornamento del software sicure
12.2	Compromissione delle procedure di aggiornamento locale/fisico del software, compresa la creazione di un falso firmware o programma di aggiornamento del sistema		
12.3	Il software è manipolato prima del processo di aggiornamento (ed è quindi corrotto), sebbene il processo di aggiornamento sia intatto		
12.4	Compromissione delle chiavi crittografiche del fornitore di software per consentire un aggiornamento non valido	M11	Devono essere effettuati controlli di sicurezza per la memorizzazione delle chiavi crittografiche
13.1	Attacco ”Denial of Service” contro un server o una rete di aggiornamento per impedire l'installazione di aggiornamenti critici del software e/o lo sblocco di funzioni specifiche del cliente	M3	Devono essere applicati controlli di sicurezza ai sistemi di back-end. Se i server di back-end sono essenziali per la fornitura dei servizi, sono previste misure di ripristino in caso di indisponibilità del sistema. Esempi di controlli di sicurezza sono reperibili in OWASP

3. Misure di attenuazione per le ”azioni umane non intenzionali che facilitano un attacco informatico”

Le misure di attenuazione delle minacce per quanto riguarda le ”azioni umane non intenzionali che facilitano un attacco informatico” sono elencate nella tabella B3.

Tabella B3

Misure di attenuazione delle minacce per quanto riguarda le ”azioni umane non intenzionali che facilitano un attacco informatico”

Riferimento tabella A1	Minacce per quanto riguarda le ”azioni umane non intenzionali”	Rif.	Misura di attenuazione
15.1	Una vittima inconsapevole (ad esempio un proprietario, un operatore o un addetto alla manutenzione) è indotta a compiere un'azione che comporta il caricamento involontario di malware o che consente un attacco	M18	Devono essere attuate misure per definire e controllare i ruoli degli utenti e i privilegi di accesso, sulla base del principio del privilegio minimo

Riferimento tabella A1	Minacce per quanto riguarda le "azioni umane non intenzionali"	Rif.	Misura di attenuazione
15.2	Le procedure di sicurezza definite non sono rispettate	M19	Le organizzazioni devono garantire che le procedure di sicurezza siano definite e rispettate, ivi compresi la registrazione delle azioni in log e l'accesso relativo alla gestione delle funzioni di sicurezza

4. Misure di attenuazione per la "connettività e collegamenti esterni"

Le misure di attenuazione delle minacce per quanto riguarda la "connettività e collegamenti esterni" sono elencate nella tabella B4.

Tabella B4

Attenuazione delle minacce per quanto riguarda la "connettività e collegamenti esterni"

Riferimento tabella A1	Minacce relative alla "connettività e collegamenti esterni"	Rif.	Misura di attenuazione
16.1	Manipolazione di funzioni progettate per comandare a distanza i sistemi dei veicoli come la chiave telecomando, l'immobilizzatore e la colonnina di carica	M20	Devono essere applicati controlli di sicurezza ai sistemi con accesso remoto
16.2	Manipolazione della telematica dei veicoli (ad esempio manipolazione della misurazione della temperatura di merci sensibili, sblocco a distanza dei portelloni di carico)		
16.3	Interferenza con sistemi o sensori senza fili a corto raggio		
17.1	Applicazioni corrotte o con scarsa sicurezza del software, utilizzate come metodo per attaccare i sistemi dei veicoli	M21	Il software deve essere sottoposto a valutazione della sicurezza, autenticato e protetto nella sua integrità. Devono essere applicati controlli di sicurezza per ridurre al minimo il rischio derivante da software di terzi destinati a essere ospitati o che si prevede saranno ospitati sul veicolo
18.1	Interfacce esterne quali USB o altre porte utilizzate come punto di attacco, ad esempio mediante iniezione di codice	M22	Devono essere applicati controlli di sicurezza alle interfacce esterne
18.2	Supporti infettati da virus collegati al veicolo		
18.3	Accesso diagnostico (ad esempio dongle nella porta OBD) utilizzato per facilitare un attacco, ad esempio per manipolare i parametri del veicolo (direttamente o indirettamente)	M22	Devono essere applicati controlli di sicurezza alle interfacce esterne

5. Misure di attenuazione per ”potenziali bersagli o motivazioni di un attacco”

Le misure di attenuazione delle minacce per quanto riguarda ”potenziali bersagli o motivazioni di un attacco” sono elencate nella tabella B5.

Tabella B5

Misure di attenuazione delle minacce per quanto riguarda ”potenziali bersagli o motivazioni di un attacco”

Riferimento tabella A1	Minacce relative a ”potenziali bersagli o motivazioni di un attacco”	Rif.	Misura di attenuazione
19.1	Estrazione di software proprietario o protetto da diritto d'autore dai sistemi dei veicoli (pirateria di prodotti/furto di software)	M7	Per proteggere il codice/i dati del sistema devono essere applicate tecniche e soluzioni per il controllo degli accessi. Esempi di controlli di sicurezza sono reperibili in OWASP
19.2	Accesso non autorizzato a informazioni private del proprietario, quali l'identità personale, le informazioni sui conti di pagamento, le informazioni sulla rubrica degli indirizzi, le informazioni relative all'ubicazione, l'ID elettronico del veicolo ecc.	M8	Attraverso la progettazione del sistema e il controllo degli accessi il personale non autorizzato non dovrebbe poter accedere ai dati personali o critici del sistema. Esempi di controlli di sicurezza sono reperibili in OWASP
19.3	Estrazione di chiavi crittografiche	M11	Devono essere effettuati controlli di sicurezza per la memorizzazione di chiavi crittografiche, ad esempio moduli di sicurezza
20.1	Modifiche illegali/non autorizzate all'ID elettronico del veicolo	M7	Per proteggere il codice/i dati del sistema devono essere applicate tecniche e soluzioni per il controllo degli accessi. Esempi di controlli di sicurezza sono reperibili in OWASP
20.2	Frode d'identità, ad esempio se un utente vuole mostrare un'altra identità quando comunica con sistemi di pedaggio o con il back-end del costruttore		
20.3	Azioni volte a eludere i sistemi di monitoraggio (ad esempio hackeraggio/ manomissione/blocco di messaggi quali i dati ODR Tracker o il numero di esecuzioni)	M7	Per proteggere il codice/i dati del sistema devono essere applicate tecniche e soluzioni per il controllo degli accessi. Esempi di controlli di sicurezza sono reperibili in OWASP Gli attacchi di manipolazione dei dati contro sensori o dati trasmessi potrebbero essere attenuati correlando i dati provenienti da diverse fonti di informazione
20.4	Manipolazione dei dati per falsificare i dati di guida del veicolo (ad esempio chilometraggio, velocità di guida, direzioni di marcia ecc.)		
20.5	Modifiche non autorizzate ai dati diagnostici del sistema		
21.1	Cancellazione/manipolazione non autorizzata dei log degli eventi di sistema	M7	Per proteggere il codice/i dati del sistema devono essere applicate tecniche e soluzioni per il controllo degli accessi. Esempi di controlli di sicurezza sono reperibili in OWASP
22.2	Introduzione di software maligni o attività di software maligni	M7	Per proteggere il codice/i dati del sistema devono essere applicate tecniche e soluzioni per il controllo degli accessi. Esempi di controlli di sicurezza sono reperibili in OWASP
23.1	Creazione di un falso software del sistema di controllo o del sistema informatico del veicolo		

Riferimento tabella A1	Minacce relative a "potenziali bersagli o motivazioni di un attacco"	Rif.	Misura di attenuazione
24.1	Attacco "Denial of Service" che può essere ad esempio innescato sulla rete interna inondando un bus CAN o provocando guasti a una centralina elettronica mediante l'invio di una grande quantità di messaggi	M13	Devono essere adottate misure per individuare e rimediare a un attacco "Denial of Service"
25.1	Accesso non autorizzato al fine di falsificare i parametri di configurazione delle funzioni chiave del veicolo, quali i dati dei freni, la soglia di attivazione dell'airbag ecc.	M7	Per proteggere il codice/i dati del sistema devono essere applicate tecniche e soluzioni per il controllo degli accessi. Esempi di controlli di sicurezza sono reperibili in OWASP
25.2	Accesso non autorizzato al fine di falsificare i parametri di carica, quali tensione di carica, potenza di carica, temperatura della batteria ecc.		

6. Misure di attenuazione per "potenziali vulnerabilità che potrebbero essere sfruttate se non sufficientemente protette o rinforzate"

Le misure di attenuazione delle minacce per quanto riguarda le "potenziali vulnerabilità che potrebbero essere sfruttate se non sufficientemente protette o rinforzate" sono elencate nella tabella B6.

Tabella B6

Misure di attenuazione delle minacce per quanto riguarda le "potenziali vulnerabilità che potrebbero essere sfruttate se non sufficientemente protette o rinforzate"

Riferimento tabella A1	Minacce relative alle "potenziali vulnerabilità che potrebbero essere sfruttate se non sufficientemente protette o rinforzate"	Rif.	Misura di attenuazione
26.1	L'uso di chiavi crittografiche brevi con un lungo periodo di validità consente agli aggressori di violare la cifratura	M23	Devono essere applicate le migliori pratiche in materia di cibersicurezza per lo sviluppo di software e hardware
26.2	Uso insufficiente di algoritmi crittografici per proteggere i sistemi sensibili		
26.3	Utilizzo di algoritmi crittografici obsoleti		
27.1	Hardware o software progettati per consentire un attacco o che non soddisfano i criteri di progettazione per fermare un attacco	M23	Devono essere applicate le migliori pratiche in materia di cibersicurezza per lo sviluppo di software e hardware
28.1	La presenza di bug del software può costituire una base per potenziali vulnerabilità sfruttabili. Ciò vale in particolare se il software non è stato testato per verificare l'assenza di codice errato/bug noti e ridurre il rischio di presenza di codice errato/bug sconosciuti	M23	Devono essere applicate le migliori pratiche in materia di cibersicurezza per lo sviluppo di software e hardware. Test di cibersicurezza con copertura adeguata

Riferimento tabella A1	Minacce relative alle "potenziali vulnerabilità che potrebbero essere sfruttate se non sufficientemente protette o rinforzate"	Rif.	Misura di attenuazione
28.2	L'utilizzo di residui dello sviluppo (ad esempio porte di debug, porte JTAG, microprocessori, certificati di sviluppo, password programmatore ecc.) può permettere agli aggressori di accedere alle centraline elettroniche o di ottenere privilegi più elevati		
29.1	Porte internet superflue lasciate aperte, che forniscono accesso ai sistemi di rete		
29.2	Elusione della separazione di rete per ottenere il controllo. Un esempio specifico è l'uso di gateway non protetti o di punti di accesso (come i gateway camion-rimorchio) per aggirare le protezioni e ottenere accesso ad altri segmenti di rete al fine di compiere atti malevoli, come l'invio di messaggi arbitrari sul bus CAN	M23	Devono essere applicate le migliori pratiche in materia di cibersicurezza per lo sviluppo di software e hardware. Devono essere applicate le migliori pratiche in materia di cibersicurezza per la progettazione e l'integrazione dei sistemi

7. Misure di attenuazione per la "perdita/violazione dei dati provenienti dal veicolo"

Le misure di attenuazione delle minacce per quanto riguarda la "perdita/violazione dei dati provenienti dal veicolo" sono elencate nella tabella B7.

Tabella B7

Misure di attenuazione delle minacce per quanto riguarda la "perdita/violazione dei dati provenienti dal veicolo"

Riferimento tabella A1	Minacce di "perdita/violazione dei dati provenienti dal veicolo"	Rif.	Misura di attenuazione
31.1	Violazione delle informazioni. I dati personali possono essere violati quando l'automobile cambia utente (ad esempio quando viene venduta o utilizzata come veicolo a noleggio con nuovi noleggiatori)	M24	Per la conservazione dei dati personali devono essere applicate le migliori pratiche in materia di protezione dell'integrità e della riservatezza dei dati.

8. Misure di attenuazione per la "manipolazione fisica dei sistemi per consentire un attacco"

Le misure di attenuazione delle minacce per quanto riguarda la "manipolazione fisica dei sistemi per consentire un attacco" sono elencate nella tabella B8.

Tabella B8

Misure di attenuazione delle minacce per quanto riguarda la "manipolazione fisica dei sistemi per consentire un attacco"

Riferimento tabella A1	Minacce relative alla "manipolazione fisica dei sistemi per consentire un attacco"	Rif.	Misura di attenuazione
32.1	Manipolazione dell'hardware OEM, ad esempio se un hardware non autorizzato è aggiunto a un veicolo per consentire un attacco "man in the middle"	M9	Devono essere adottate misure per prevenire e individuare l'accesso non autorizzato

PARTE C.

Misure di attenuazione delle minacce esterne ai veicoli

1. Misure di attenuazione per i "server di back-end"

Le misure di attenuazione delle minacce per quanto riguarda i "server di back-end" sono elencate nella tabella C1.

Tabella C1

Misure di attenuazione delle minacce per quanto riguarda i "server di back-end"

Riferimento tabella A1	Minacce ai "server di back-end"	Rif.	Misura di attenuazione
1.1 & 3.1	Abuso di privilegi da parte del personale (attacco dall'interno)	M1	Sono applicati controlli di sicurezza ai sistemi di back-end per ridurre al minimo il rischio di attacchi dall'interno
1.2 & 3.3	Accesso internet non autorizzato al server (attivato ad esempio tramite backdoor, vulnerabilità del software di sistema non corrette tramite patch, attacchi SQL o altri mezzi)	M2	Sono applicati controlli di sicurezza ai sistemi di back-end per ridurre al minimo gli accessi non autorizzati. Esempi di controlli di sicurezza sono reperibili in OWASP
1.3 & 3.4	Accesso fisico non autorizzato al server (effettuato ad esempio mediante chiavette USB o altri supporti che si collegano al server)	M8	Attraverso la progettazione del sistema e il controllo degli accessi il personale non autorizzato non dovrebbe poter accedere ai dati personali o critici del sistema
2.1	L'attacco al server di back-end ne blocca il funzionamento, ad esempio impedendogli di interagire con i veicoli e di fornire i servizi su cui questi ultimi fanno affidamento	M3	Sono applicati controlli di sicurezza ai sistemi di back-end. Se i server di back-end sono essenziali per la fornitura dei servizi, sono previste misure di ripristino in caso di indisponibilità del sistema. Esempi di controlli di sicurezza sono reperibili in OWASP
3.2	Perdita di informazioni nel cloud. I dati sensibili conservati presso fornitori terzi di servizi cloud possono andare perduti a causa di attacchi o incidenti	M4	Sono applicati controlli di sicurezza per ridurre al minimo i rischi associati al cloud computing. Esempi di controlli di sicurezza sono reperibili negli orientamenti in materia di cloud computing OWASP e NCSC
3.5	Violazione delle informazioni dovuta alla condivisione non intenzionale dei dati (ad esempio errori amministrativi, conservazione dei dati in server all'interno di garage)	M5	Sono applicati controlli di sicurezza ai sistemi di back-end per prevenire violazioni dei dati. Esempi di controlli di sicurezza sono reperibili in OWASP

2. Misure di attenuazione per le "azioni umane non intenzionali"

Le misure di attenuazione delle minacce per quanto riguarda le "azioni umane non intenzionali" sono elencate nella tabella C2.

Tabella C2

Misure di attenuazione delle minacce per quanto riguarda le "azioni umane non intenzionali"

Riferimento tabella A1	Minacce per quanto riguarda le "azioni umane non intenzionali"	Rif.	Misura di attenuazione
15.1	Una vittima inconsapevole (ad esempio un proprietario, un operatore o un addetto alla manutenzione) è indotta a compiere un'azione che comporta il caricamento involontario di malware o che consente un attacco	M18	Devono essere attuate misure per definire e controllare i ruoli degli utenti e i privilegi di accesso, sulla base del principio del privilegio minimo
15.2	Le procedure di sicurezza definite non sono rispettate	M19	Le organizzazioni devono garantire che le procedure di sicurezza siano definite e rispettate, ivi compresi la registrazione delle azioni in log e l'accesso relativo alla gestione delle funzioni di sicurezza

3. Misure di attenuazione per la "perdita fisica di dati"

Le misure di attenuazione delle minacce per quanto riguarda la "perdita fisica di dati" sono elencate nella tabella C3.

Tabella C3

Misure di attenuazione delle minacce per quanto riguarda la "perdita fisica di dati"

Riferimento tabella A1	Minacce di "perdita fisica di dati"	Rif.	Misura di attenuazione
30.1	Danni causati da terzi. I dati sensibili possono andare perduti o essere compromessi a causa di danni fisici in caso di incidente stradale o furto	M24	Per la conservazione dei dati personali devono essere applicate le migliori pratiche in materia di protezione dell'integrità e della riservatezza dei dati. Esempi di controlli di sicurezza sono reperibili in ISO/SC27/WG5
30.2	Perdite derivanti da conflitti di DRM (Digital Right Management, gestione dei diritti digitali). I dati dell'utente possono essere cancellati a causa di problemi di DRM		
30.3	I dati sensibili (o la loro integrità) possono andare perduti a causa dell'usura dei componenti informatici, comportando potenziali problemi a cascata (ad esempio in caso di alterazione della chiave)		