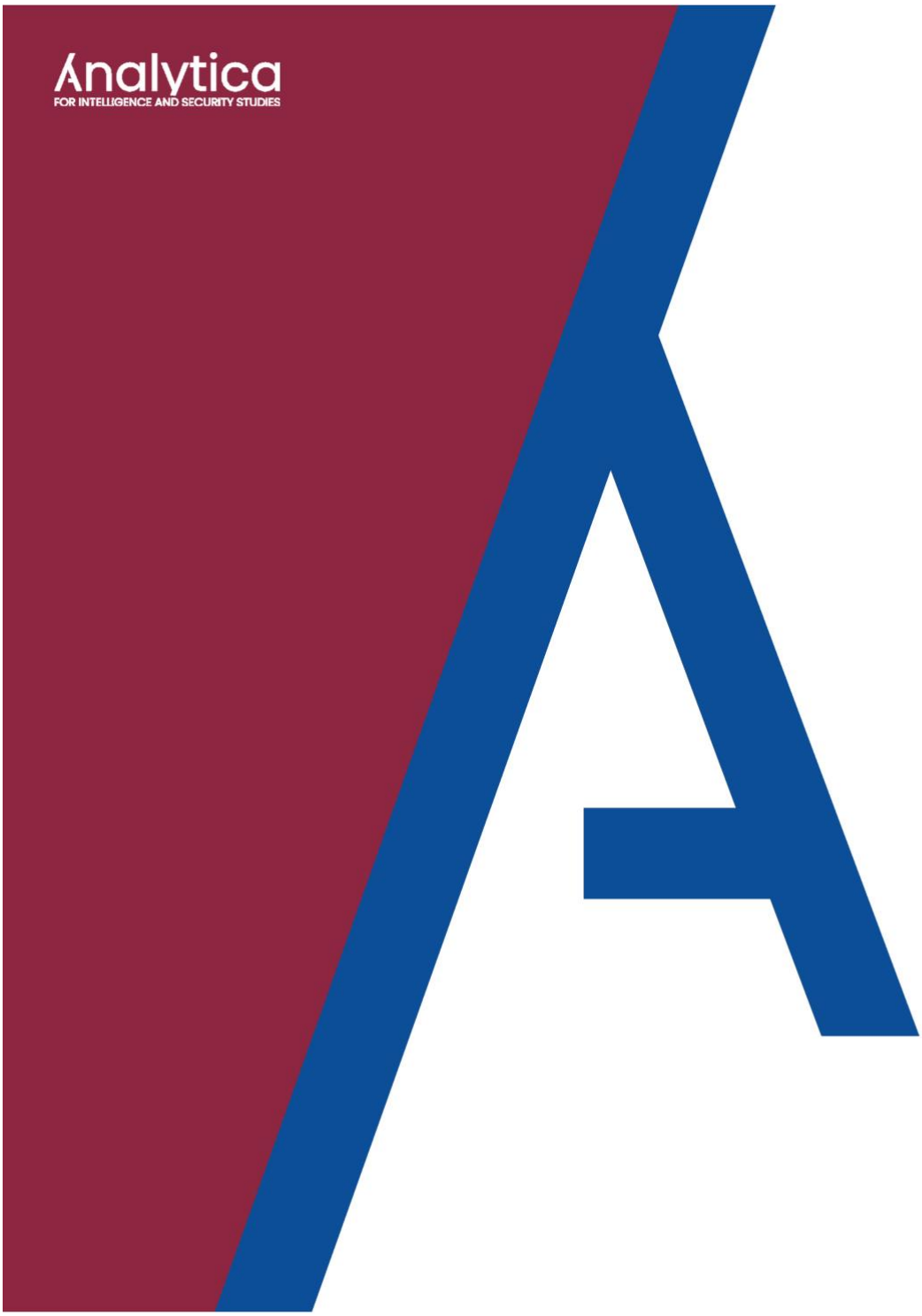

La minaccia cyber alle supply chain: il caso Kaseya VSA.

Giulia Molinari

Analytica for intelligence and security studies

Paper Cyber-Security

ISSN: 2784-8779

La minaccia cyber alle supply chain: il caso Kaseya VSA.

Giulia Molinari

Correzioni e revisioni a cura del Dottor FERAZZA Francesco

Senior Analist dipartimento Cyber - Security

Torino, luglio 2021

Il processo di digitalizzazione che da circa vent'anni sta interessando tutti gli ambiti delle società in cui viviamo ha portato con sé non solo straordinari miglioramenti ma anche numerosi nuovi rischi. Sempre più frequenti, infatti, sono i cyber-attacchi ai danni delle aziende: dalle più piccole alle multinazionali, moltissime organizzazioni dimostrano di non essere adeguatamente preparate a fronteggiare le minacce cibernetiche. I principali strumenti adottati dai criminali in rete sono detti *malware*, ossia software malevoli utilizzati con lo scopo di danneggiare un sistema. All'interno di questa ampia categoria si trovano i *ransomware,* i quali, criptando i file presenti all'interno di un dispositivo o sistema, permettono ai cybercriminali di richiedere alle proprie vittime il pagamento di un riscatto per rimuovere le limitazioni.

È a questa seconda tipologia che appartiene il software utilizzato dal gruppo di hacker russi REvil per sferrare un attacco cibernetico lo scorso venerdì 2 luglio. L'evento rappresenta un interessante caso di analisi poiché si tratta di un attacco ad una *supply chain* che ha interessato diverse aziende in tutto il mondo.

L'attacco cyber

Nel pomeriggio di venerdì 2 luglio 2021, appena prima del fine settimana di festeggiamenti per la Festa del Ringraziamento, l'azienda statunitense Kaseya ha notificato i suoi clienti in merito ad un attacco *ransomware* contro il proprio software VSA.

Kaseya, con sede a Miami, Florida, è una piattaforma in cloud che fornisce software per il monitoraggio e la gestione delle infrastrutture IT da remoto. Il gruppo di hacker ha identificato e sfruttato delle vulnerabilità *zero-day*[1] presenti nel software per sferrare un attacco non solo contro l'azienda colpita direttamente, ma interessando una buona parte del *network* dei clienti di Kaseya. La portata di un attacco di tipo *supply chain* è tale da far sì che le vittime del *ransomware* siano sparse in tutto il mondo, senza esclusione dell'Italia.

Dal punto di vista tecnico, per quanto concerne il caso Kaseya, il gruppo REvil ha distribuito il file agent.crt sotto forma di aggiornamento del software con il nome di 'Kaseya VSA Agent Hot-fix'. All'apertura del file malevolo, è stato lanciato un comando di PowerShell che ha disabilitato alcune funzionalità di sicurezza di Microsoft Defender. Successivamente, il file agent.crt è stato decodificato attraverso il comando Windows certutil.exe per l'estrazione del file agent.exe, responsabile del processo di criptazione.

[1] "Vulnerabilità riferite a sistemi, apparati e applicazioni non ancora note al produttore della tecnologia." https://csirt.gov.it/glossario/115

Poco dopo l'attacco, sul dark web è stata pubblicata dal gruppo REvil la richiesta di pagamento di un riscatto di 70 milioni di dollari in bitcoin per il rilascio della chiave di decrittazione. La somma, se fosse stata pagata, sarebbe stata la più alta cifra mai chiesta per un *ransomware*. Finora, sembrerebbe che il gruppo REvil non abbia anche sottratto dei dati dai computer infettati, che gli avrebbero permesso di attuare una *double extortion*, ossia una doppia richiesta di riscatto per evitare la pubblicazione sul *dark web* dei dati esfiltrati.

Il caso Kaseya VSA è particolarmente interessante perché la situazione di vulnerabilità psicologica delle vittime è stata subito sfruttata per sferrare un secondo attacco, questa volta sotto forma di campagna di spam *malware*.

Martedì 6 luglio, infatti, solo quattro giorni dopo il primo attacco, *Malwarebites Threat Intelligence* ha pubblicato un tweet di allerta in merito a un finto aggiornamento di sicurezza Microsoft che avrebbe dovuto mitigare la vulnerabilità di Kaseya che aveva permesso agli hacker di attuare il primo attacco. L'apertura del link o dell'allegato con il nome di 'SecurityUpdates.exe' presenti nella email lancerebbe CobaltStrike, usato per ottenere l'accesso da remoto dei sistemi infettati. CobaltStrike è un software utilizzato legittimamente per effettuare dei test di penetrazione: attraverso la simulazione di un attacco permette di identificare le vulnerabilità di un sistema informatico. Tuttavia, il suo utilizzo per scopi illeciti ha registrato un'impennata del 161% tra il 2019 e il 2020[2], dimostrandosi una valida alternativa ai *trojan*. Dopo la fuga di notizie che ha rivelato il codice sorgente del software nel novembre 2020, i cybercriminali hanno, infatti, trovato un modo per utilizzarlo illegalmente per esfiltrare dati, lanciare *malware* e creare dei profili falsi di *command-and-control* (C2) apparentemente regolari che sfuggono ai software di sicurezza.

Un altro avviso di allerta è stato anche pubblicato dalla stessa Kaseya l'8 luglio in merito ad una campagna di phishing via email e chiamate telefoniche attraverso le quali i criminali si fingevano dei partner dell'azienda che offrivano supporto ai clienti in seguito al primo attacco *ransomware* del 2 luglio.

[2] https://threatpost.com/cobalt-strike-cybercrooks/167368/

Contromisure adottate da Kaseya

Così come accadde già lo scorso anno con l'attacco al *service provider* SolarWinds, anche questo crimine cibernetico non ha interessato una sola vittima ma ha avuto effetti su aziende in tutto il mondo. Questo tipo di attacchi, che sta diventando sempre più frequente, si concentra su un *provider* che fornisce ai suoi clienti un servizio - nel caso di Kaseya, un software per il monitoraggio e la gestione da remoto delle infrastrutture IT -, riuscendo con un solo colpo a danneggiare l'intera *supply chain*.

Sin dalle prime ore successive all'incidente, l'azienda statunitense ha pubblicato sul suo sito[3] frequenti aggiornamenti in merito alle contromisure adottate. Per prima cosa, il team di *Incident Response* ha raccomandato di spegnere tutti i server VSA *on-premise*, per poi procedere con lo spegnimento preventivo anche dei server *Software-as-a-Service* (SaaS) nonostante non fossero stati interessati dall'attacco. Parallelamente, è stato avviato il processo vero e proprio di risposta all'incidente, ossia le indagini per comprenderne la causa e la notifica alle autorità competenti, come l'FBI e il CISA (*Cybersecurity and Infrastructure Security Agency*). Questa prima fase di risposta, come dichiarato anche dal CEO dell'azienda Fred Voccola, è stata efficace e tempestiva, e ha permesso di limitare il numero di vittime a circa 60 clienti diretti di Kaseya e 1500 organizzazioni a loro collegate.

Dal 3 luglio, gli aggiornamenti forniti dall'azienda si sono divisi seguendo due obiettivi, ossia il ripristino del servizio e l'assistenza ai propri clienti. Per quanto riguarda la *Business Continuity*, l'azienda si è mossa per replicare il vettore del *ransomware* e valutarne l'impatto, e per identificare i cosiddetti IoC (*Indicators of Compromise*), o indicatori di compromissione, per l'elaborazione di uno strumento di auto-valutazione che permettesse ai clienti di sapere se i propri sistemi fossero stati interessati dall'attacco. Per quanto concerne invece la *customer care*, l'azienda ha continuato a raccomandare di tenere spenti sia i server VSA che quelli SaaS fino a nuovo avviso, e comunque non prima del rilascio di una *patch.*

Durante la notte tra il 3 e il 4 luglio, è stato lanciato il *Compromise Detection Tool*: si tratta di uno strumento messo a disposizione dei clienti di Kaseya che ne facevano richiesta via email utile per determinare se i propri server fossero stati colpiti dal *ransomware*. L'elaborazione di tale strumento è stata possibile grazie allo studio condotto dal team R&D per l'identificazione degli IoC.

---

[3] https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-July-2nd-2021 ultima data di consultazione: 12 luglio 2021.

Nel pomeriggio del 4 luglio, due giorni dopo l'attacco, Kaseya ha anche annunciato la *timeline* per il ripristino del servizio dei server SaaS, i quali, si rammenta, non erano stati interessati dall'incidente ma erano stati ugualmente spenti per precauzione. Il riavvio dei server VSA *on-premise*, ossia il target dell'attacco informatico, era previsto solo dopo aver portato a termine con successo l'accensione dei SaaS e comunque non prima del rilascio dell'apposita *patch*. Secondo i piani, il processo di riavvio dei server SaaS sarebbe dovuto iniziare il 5 luglio, prima per quelli in UE, UK e Asia Pacifica, per poi procedere con il Nord America.

Tuttavia, la procedura di ripristino dei server è stata interrotta poiché il comitato esecutivo ha deliberato che fosse necessario più tempo per minimizzare al meglio i rischi. Il 5 luglio, Kaseya ha fissato il riavvio dei server SaaS per il pomeriggio del giorno seguente, riservandosi, però, di annunciare la decisione definitiva durante la mattina del 6 luglio in base ai risultati del collaudo finale e dei processi di validazione. Questi slittamenti dell'avvio della procedura hanno causato un ritardo anche nel riavvio dei server VSA interessati dall'incidente, previsto in seguito al ripristino dei server SaaS. Nella sera di martedì 6 luglio, Kaseya ha annunciato l'inizio del processo. Tuttavia, dopo solo un'ora dall'avvio, l'azienda ha notificato l'interruzione della procedura a causa di un problema emerso durante l'installazione, rassicurando i propri clienti che avrebbe fatto il possibile per ripristinare il servizio entro giovedì 8 luglio. Nel mentre, il team di R&D ha ultimato la stesura dei *runbook* con le procedure necessarie da seguire per prepararsi al riavvio dei server SaaS e per l'installazione della *patch* per i clienti con server VSA *on-premise*. Nel pomeriggio di giovedì 8 luglio, Kaseya ha annunciato che le procedure di riavvio dei server SaaS e il rilascio della *patch* per i server VSA *on-premise* sarebbero iniziate entrambe domenica 11 luglio. A differenza dei primi due tentativi, in questo caso Kaseya è riuscita a ripristinare i propri servizi, sia per quanto riguarda il riavvio dei server SaaS spenti per precauzione, che in merito al rilascio della *patch* per i server VSA. I team di assistenza sono rimasti operativi per tutta la durata della procedura e hanno continuato a prestare supporto ai clienti che hanno riscontrato difficoltà.

Lunedì 12 i server SaaS sono stati fuori servizio per circa venti minuti a causa del grande numero di utenti che sono tornati online contemporaneamente. L'azienda ha definito questo problema un '*performance issue*' che non sarebbe quindi legato a problematiche tecniche ma solamente dovuto a un sovraccarico di utenze. Tutto è stato comunque risolto in poche ore. L'azienda ha dichiarato il completamento delle procedure di ripristino dei suoi servizi nel pomeriggio di lunedì 12 luglio. Ad ogni modo, ha garantito che continuerà a monitorare le prestazioni dei server e ad apportare modifiche laddove necessario.

Parallelamente agli aggiornamenti giornalieri riguardanti le contromisure all'attacco *ransomware*, un ulteriore avvertimento è stato pubblicato dall'azienda nella sera dell'8 luglio: molti casi di *phishing*, infatti, sono stati registrati ai danni dei clienti del *provider* mediante una campagna spam email di finti aggiornamenti di Kaseya con link e allegati malevoli che avrebbero lanciato CobaltStrike. Il giorno seguente, l'azienda ha notificato che i cybercriminali avevano anche effettuato delle chiamate telefoniche fingendosi dei partner di Kaseya che contattavano i clienti per offrire supporto.

Gestione dell'incidente in Italia

Trattandosi di un incidente informatico di tipo *supply chain*, le aziende interessate non sono confinate solo al territorio degli Stati Uniti ma bensì sono sparse in tutto il mondo. Infatti, anche alcune organizzazioni italiane sono state vittime del *ransomware*. Così come Kaseya ha notificato l'incidente alle autorità competenti statunitensi, nello specifico il CISA e l'FBI, le aziende nei paesi membri dell'Unione Europea fanno invece riferimento al CSIRT (*Computer Security Incident Response Team*) locale. L'istituzione di questi gruppi di esperti ha origine dalla direttiva (UE) 2016/1148 del Parlamento e del Consiglio Europeo, la quale ha dato impulso alla creazione di una rete di collaborazione tra i membri dell'Unione in materia di sicurezza cibernetica. Il CSIRT italiano è stato costituito con il Decreto Legislativo 18 maggio 2018, n. 65, e con il Decreto del Presidente del Consiglio dei Ministri Giuseppe Conte dell'8 agosto 2019. Analogamente ai compiti del CISA, il CSIRT si occupa di monitorare e intervenire in caso di attacchi cibernetici a livello nazionale, emettere allerte e annunci, condurre analisi dinamiche di rischi e incidenti, sensibilizzare la popolazione sulla cybersicurezza, e collaborare con i CSIRT presenti negli altri paesi membri dell'UE. L'obbligo di notifica di incidente informatico riguarda, però, solo alcune determinate categorie di aziende, nello specifico gli Operatori di Servizi Essenziali (OSE), i Fornitori di Servizi Digitali (FSD) e gli operatori di reti e sistemi di comunicazioni elettroniche (TELCO). Non trattandosi di aziende appartenenti a queste categorie, le organizzazioni italiane che fanno parte della *supply chain* colpita dal gruppo REvil non avevano l'obbligo di notificare l'attacco al CSIRT. Tuttavia, è interessante evidenziare il ruolo che questo organo ha avuto in relazione ai suoi compiti di emissione di allerte e annunci, e di analisi dinamica degli incidenti.

Il 5 luglio scorso, tre giorni dopo l'individuazione del *ransomware* in esame, il CSIRT[4] ha pubblicato un alert a riguardo. L'avviso riportava prima di tutto la notizia dell'incidente con una breve descrizione dell'evento e dei suoi potenziali impatti; ma non si limitava a questo. L'avviso, infatti, sottolineava anche l'importanza di seguire le raccomandazioni che Kaseya aveva fin da subito fatto ai suoi clienti, ossia di mantenere spenti i server VSA e di verificare con l'apposito *tool* l'eventuale presenza di IoC (*indicators of compromise*). Inoltre, il CSIRT ha anche consigliato ulteriori contromisure per aumentare il livello di sicurezza cibernetica delle aziende. In particolare, ha suggerito l'implementazione dell'autenticazione forte o multifattore (MFA), l'utilizzo di una connessione VPN per proteggere l'accesso alle infrastrutture di *Remote Management and Monitoring* (RMM), la conservazione di backup aggiornati in forma fisica o disconnessi dalle reti aziendali, la gestione manuale del processo di installazione delle *patch* fino alla risoluzione del problema, l'implementazione del modello *least privilege*[5] sugli account aziendali, e l'inserimento di alcuni IoC (*indicators of compromise*) nei sistemi di sicurezza.

Analisi della gestione dell'incidente

Come dichiarato dal CEO di Kaseya, Fred Voccola, le prime fasi di risposta all'attacco sono state tempestive e proattive. L'immediato spegnimento dei server VSA *on-premise* presi di mira dai criminali e l'interruzione preventiva del servizio SaaS hanno permesso di limitare notevolmente il numero di server infettati. Tuttavia, come si evince dalla *timeline* precedentemente illustrata, il ripristino del servizio ha richiesto tempi eccessivamente lunghi che hanno causato importanti danni e problemi non solo a Kaseya, ma anche a tutti i suoi clienti MSP e alle aziende a loro connesse.

Già in occasione dei recenti attacchi a SolarWinds e a Microsoft Exchange, i piani di *Business Continuity* e *Disaster Recovery* si erano dimostrati inappropriati per fronteggiare attacchi di tale portata. In particolare, questi due piani consistono in una serie prefissata di procedure da attuare per permettere la continuità del servizio in caso di incidenti informatici o di altra natura e per ripristinare gli *asset* danneggiati. Al contrario, il piano di *Incident Handling*, ossia la gestione dell'incidente, è stato messo in moto fin da subito, permettendo, così, di limitare il numero di vittime.

---

[4] https://csirt.gov.it/contenuti/attacco-ransomware-alla-piattaforma-software-vsa-di-kaseya-al01-210705-csirt-ita

[5] Con il termine *least privilege* o minimo privilegio si intende il principio per cui ogni utente, account, o programma deve avere solo il minimo accesso a sistemi o risorse che gli sia sufficiente a svolgere il proprio lavoro.

È importante menzionare che in caso di attacchi *ransomware*, il pagamento del riscatto richiesto dal gruppo di hacker dovrebbe essere l'ultima possibilità da prendere in considerazione per diversi motivi. In primo luogo, il pagamento della somma richiesta non garantisce il rilascio della chiave di decrittazione. Inoltre, è sempre più frequente che i criminali esfiltrino i dati prima di criptarli per poter chiedere un doppio riscatto, prima per decrittare i file e dopo per evitarne la pubblicazione sui cosiddetti *leak site*[6] sul dark web. Anche in questo caso, il pagamento della somma richiesta non garantisce che i criminali rispettino gli accordi.

CONCLUSIONI

Nonostante siano sempre più frequenti gli attacchi di tipo cibernetico, moltissime organizzazioni si dimostrano impreparate alla gestione degli incidenti informatici. In particolare, la diffusione dei *ransomware* preoccupa non solo le piccole aziende, ma anche e soprattutto le multinazionali e i fornitori di servizi. Come già avvenuto ai danni di SolarWinds e di Microsoft Exchange, anche l'attacco sferrato contro i server VSA *on-premise* di Kaseya non ha interessato solo l'azienda statunitense ma anche molti suoi clienti e le organizzazioni a loro collegate. Questo tipo di strategia è di tipo *supply chain*: colpendo il *provider* di un servizio si producono effetti a cascata sull'intero *network* dei suoi clienti.

Di vitale importanza per le aziende, è, pertanto, la predisposizione di contromisure efficaci da attuare in caso di incidenti informatici e non che permettano la continuità del servizio e un rapido ripristino degli *asset* danneggiati. Questi piani hanno il nome di *Incident Handling and Response*, *Business Continuity*, *Disaster Recovery* e *patch management*. In diverse occasioni, come ad esempio nel caso dell'attacco a Kaseya, la tempestiva decisione di spegnere tutti i server VSA *on-premise* e SaaS ha permesso di limitare notevolmente il numero di vittime. Tuttavia, la risoluzione del problema dal punto di vista tecnico e il ripristino del servizio hanno richiesto diversi giorni, creando danni e interruzioni non solo del servizio fornito da Kaseya, ma anche dei servizi erogati dai suoi clienti a terzi.

Per prima cosa, tutte quelle organizzazioni che fanno uso di mezzi digitali è bene che si assicurino sia di garantire la sicurezza dei dati (e.g., backup aggiornati ed *air-gapped*), delle reti (e.g., VPN, segregazione dei network), e dei sistemi (e.g., aggiornandoli), che di implementare metodi di autenticazione forte (e.g., MFA).

[6] Siti nel dark web dove vengono pubblicati i dati ottenuti prima della criptazione in caso di mancato pagamento del riscatto.

In aggiunta a questi accorgimenti che dovrebbero ormai essere basilari, è importante che le aziende abbiano piena visibilità e conoscenza dei propri *asset* tecnologici per facilitare e velocizzare l'identificazione, la valutazione e la gestione dei rischi a cui esse sono esposte. Inoltre, non si dovrebbe sottovalutare l'importanza di individuare e correggere tempestivamente le vulnerabilità, rinforzare i punti deboli, e predisporre adeguati piani di contromisure e recupero dell'operatività da mettere in pratica in caso di - inevitabili - incidenti di sicurezza.