EBA/GL/2017/17

12/01/2018

Orientamenti

sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento ai sensi della direttiva (UE) 2015/2366 (PSD2)

1. Conformità e obblighi di comunicazione

Status giuridico degli orientamenti

1. Il presente documento contiene orientamenti emanati in applicazione dell'articolo 16 del regolamento (UE) n. 1093/2010[1]. Conformemente all'articolo 16, paragrafo 3, del regolamento (UE) n. 1093/2010, le autorità competenti e gli enti finanziari compiono ogni sforzo per conformarsi agli orientamenti.

2. Gli orientamenti presentano la posizione dell'ABE in merito alle prassi di vigilanza adeguate all'interno del Sistema europeo di vigilanza finanziaria o alle modalità di applicazione del diritto dell'Unione in un particolare settore. Ai sensi dell'articolo 4, paragrafo 2, del regolamento (UE) n. 1093/2010, le autorità competenti sono tenute a conformarsi a detti orientamenti integrandoli opportunamente nelle rispettive prassi di vigilanza (per esempio modificando il proprio quadro giuridico o le proprie procedure di vigilanza), anche quando gli orientamenti sono diretti principalmente agli enti.

Obblighi di comunicazione

3. Ai sensi dell'articolo 16, paragrafo 3, del regolamento (UE) n. 1093/2010, le autorità competenti devono comunicare all'ABE entro 12.03.2018 se sono conformi o se intendono conformarsi agli orientamenti in questione; in alternativa sono tenute a indicare le ragioni della mancata conformità. Qualora entro il termine indicato non sia pervenuta alcuna comunicazione da parte delle autorità competenti, queste sono ritenute dall'ABE non conformi. Le notifiche dovrebbero essere inviate trasmettendo il modulo disponibile sul sito web dell'ABE all'indirizzo compliance@eba.europa.eu con il riferimento "EBA/GL/2017/17" da persone debitamente autorizzate a segnalare la conformità per conto delle rispettive autorità competenti. Ogni eventuale variazione dello status di conformità deve essere altresì comunicata all'ABE.

4. Le comunicazioni sono pubblicate sul sito web dell'ABE ai sensi dell'articolo 16, paragrafo 3.

[1] Regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità bancaria europea), modifica la decisione 716/2009/CE e abroga la decisione 2009/78/CE della Commissione (GU L 331 del 15.12.2010, pag. 12).

2. Oggetto, ambito di applicazione e definizioni

Oggetto e ambito di applicazione

5. I presenti orientamenti sono stati redatti in virtù del mandato conferito all'ABE ai sensi dell'articolo 95, paragrafo 3, della direttiva (UE) 2015/2366[2] (PSD2).

6. I presenti orientamenti specificano i requisiti per la definizione, l'attuazione e il monitoraggio delle misure di sicurezza che i prestatori di servizi di pagamento devono adottare ai sensi dell'articolo 95, paragrafo 1, della direttiva (UE) 2015/2366 per gestire i rischi operativi e di sicurezza relativi ai servizi di pagamento che prestano.

Destinatari

7. I presenti orientamenti sono destinati ai prestatori di servizi di pagamento quali definiti nell'articolo 4, paragrafo 11, della direttiva (UE) 2015/2366 e citati nella definizione di «istituti finanziari» di cui all'articolo 4, paragrafo 1, del regolamento (UE) 1093/2010, nonché alle autorità competenti quali definite nell'articolo 4, paragrafo 2, punto i), dello stesso regolamento, con riferimento alla direttiva abrogata 2007/64/CE[3] [attualmente direttiva (UE) 2015/2366[4]].

Definizioni

8. Se non diversamente specificato, i termini utilizzati e definiti nella direttiva (UE) 2015/2366 hanno il medesimo significato nei presenti orientamenti. Inoltre, ai fini dei presenti orientamenti si applicano le seguenti definizioni.

[2] Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE (GU L 337 del 23.12.2015, pag. 35).
[3] Direttiva 2007/64/CE del Parlamento europeo e del Consiglio, del 13 novembre 2007, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE, che abroga la direttiva 97/5/CE (GU L 319 del 5.12.2007, pag. 1).
[4] Ai sensi dell'articolo 114, secondo comma, della direttiva (UE) 2015/2366, i riferimenti alla direttiva abrogata 2007/64/CE si intendono fatti alla direttiva (UE) 2015/2366 e si leggono secondo la tavola di concordanza di cui all'allegato II della direttiva (UE) 2015/2366.

Organo di gestione	– Per i prestatori di servizi di pagamento che sono istituti di credito, questo termine ha il medesimo significato di cui alla definizione dell'articolo 3, paragrafo 1, punto 7), della direttiva 2013/36/UE[5]. – Per i prestatori di servizi di pagamento che sono istituti di pagamento o istituti di moneta elettronica, questo termine indica i direttori o le persone responsabili della gestione del prestatore di servizi di pagamento e, laddove opportuno, le persone responsabili della gestione delle attività connesse ai servizi di pagamento del prestatore di tali servizi. – Per i prestatori di servizi di pagamento di cui all'articolo 1, paragrafo 1, lettere c), e) ed f), della direttiva (UE) 2015/2366, questo termine ha il significato che gli viene attribuito dalla normativa nazionale o dell'UE applicabile.
Incidente operativo o di sicurezza	Singolo evento o serie di eventi collegati, non pianificati dal prestatore di servizi di pagamento che ha, o probabilmente avrà, un impatto negativo sull'integrità, la disponibilità, la riservatezza, l'autenticità e/o la continuità dei servizi relativi ai pagamenti.
Alta dirigenza	(a) Per i prestatori di servizi di pagamento che sono istituti di credito, questo termine ha il medesimo significato di cui alla definizione dell'articolo 3, paragrafo 1, punto 9), della direttiva 2013/36/UE. (b) Per i prestatori di servizi di pagamento che sono istituti di pagamento o istituti di moneta elettronica, questo termine indica le persone fisiche che esercitano funzioni esecutive, sono responsabili della gestione quotidiana del prestatore di servizi di pagamento e ne devono rispondere all'organo di gestione. (c) Per i prestatori di servizi di pagamento di cui all'articolo 1, paragrafo 1, lettere c), e) ed f), della direttiva (UE) 2015/2366, questo termine ha il significato che gli viene attribuito dalla normativa nazionale o dell'UE applicabile.
Rischio di sicurezza	Il rischio derivante dall'inadeguatezza o dalla mancanza di processi interni oppure da eventi esogeni che hanno, o potrebbero avere, un effetto negativo sulla disponibilità, integrità e riservatezza dei sistemi che impiegano le tecnologie dell'informazione e della comunicazione (ICT) e/o delle informazioni utilizzate per la prestazione dei servizi di pagamento. È compreso il rischio derivante da attacchi informatici o da un livello inadeguato di sicurezza fisica.

[5] Direttiva 2013/36/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE (GU L 176 del 27.6.2013, pag. 338).

Propensione al rischio	Il livello complessivo e i tipi di rischio che un ente è disposto ad assumere per conseguire gli obiettivi strategici che si è prefissato, in funzione della sua capacità di tollerare il rischio in linea con il suo modello di business.

3. Attuazione

Data di applicazione

9. I presenti orientamenti si applicano a partire dal 13 gennaio 2018.

4. Orientamenti

Orientamento 1: Principio generale

1.1 Tutti i prestatori di servizi di pagamento dovrebbero essere conformi a tutte le disposizioni di cui ai presenti orientamenti. Il livello di dettaglio dovrebbe essere proporzionato alle dimensioni del prestatore di servizi di pagamento, nonché alla natura, allo scopo, alla complessità e alla rischiosità dei particolari servizi che egli presta o intende prestare.

Orientamento 2: Governance

Framework per la gestione dei rischi operativi e di sicurezza

2.1 I prestatori di servizi di pagamento dovrebbero definire un framework di riferimento efficace per la gestione dei rischi operativi e di sicurezza (di seguito «framework per la gestione dei rischi») che dovrebbe essere approvato e riesaminato almeno a cadenza annuale dall'organo di gestione e, se del caso, dall'alta dirigenza. Tale framework dovrebbe concentrarsi sulle misure di sicurezza per mitigare i rischi operativi e di sicurezza e dovrebbe essere pienamente integrato nei processi globali di gestione dei rischi del prestatore di servizi di pagamento.

2.2 Il framework per la gestione dei rischi dovrebbe:

a) comprendere un esauriente documento relativo alla politica di sicurezza quale indicato nell'articolo 5, paragrafo 1, lettera j), della direttiva (UE) 2015/2366;

b) essere coerente con la propensione al rischio del prestatore di servizi di pagamento;

c) definire e attribuire i ruoli e le responsabilità fondamentali, nonché le pertinenti linee di riporto gerarchico necessarie per rafforzare le misure di sicurezza e gestire i rischi operativi e di sicurezza;

d) stabilire le procedure e i sistemi necessari per individuare, misurare, monitorare e gestire la gamma di rischi derivanti dalle attività connesse ai servizi di pagamento svolte dal prestatore di servizi di pagamento e ai quali esso è esposto, comprese le disposizioni in materia di continuità operativa.

2.3 I prestatori di servizi di pagamento dovrebbero garantire che il framework per la gestione dei rischi sia adeguatamente documentato, e inoltre aggiornato sulla base di quanto appreso e formalizzato durante l'applicazione e il monitoraggio.

2.4 I prestatori di servizi di pagamento dovrebbero verificare la necessità di modificare o migliorare senza indebiti ritardi il framework per la gestione dei rischi prima di una modifica sostanziale delle infrastrutture, dei processi o delle procedure e dopo ogni incidente operativo o di sicurezza grave che pregiudichi la sicurezza dei servizi di pagamento da essi prestati.

Modelli di gestione e controllo dei rischi

2.5 I prestatori di servizi di pagamento dovrebbero definire tre linee di difesa efficaci oppure un equivalente modello interno di gestione e controllo dei rischi per individuare e gestire i rischi operativi e di sicurezza. I prestatori di servizi di pagamento dovrebbero garantire che il summenzionato modello interno di controllo disponga di sufficienti autorità, autonomia, risorse e linee di rendicontazione dirette con l'organo di gestione e, se del caso, con l'alta dirigenza.

2.6 Le misure di sicurezza di cui ai presenti orientamenti dovrebbero essere esaminate da revisori competenti in materia di sicurezza informatica e pagamenti, interni o esterni, operativamente indipendenti dal prestatore di servizi di pagamento. La frequenza e il contenuto di questi controlli dovrebbero tenere conto dei relativi rischi di sicurezza.

Esternalizzazione

2.7 I prestatori di servizi di pagamento dovrebbero garantire l'efficacia delle misure di sicurezza di cui ai presenti orientamenti in caso di esternalizzazione delle funzioni operative dei servizi di pagamento, compresi i sistemi informatici.

2.8 I prestatori di servizi di pagamento dovrebbero garantire che i contratti e gli accordi di livello del servizio conclusi con i prestatori ai quali hanno esternalizzato tali funzioni contemplino obiettivi, misure e prestazioni adeguate e proporzionate in materia di sicurezza. I prestatori di servizi di pagamento dovrebbero monitorare e ottenere garanzie per quanto riguarda il livello di conformità dei suddetti fornitori agli obiettivi, alle misure e alle prestazioni di sicurezza.

Orientamento 3: Valutazione dei rischi

Individuazione delle funzioni, dei processi e delle risorse

3.1 I prestatori di servizi di pagamento dovrebbero individuare, definire e aggiornare periodicamente un inventario delle funzioni aziendali, dei ruoli fondamentali e dei processi di supporto, al fine di identificare l'importanza di ciascuna funzione, ruolo e processo di supporto, nonché le loro interdipendenze in materia di rischi operativi e di sicurezza.

3.2 I prestatori di servizi di pagamento dovrebbero individuare, definire e aggiornare periodicamente un inventario delle risorse informatiche, come i sistemi ICT, le loro configurazioni, altre infrastrutture nonché le interconnessioni con altri sistemi interni ed esterni, per poter gestire le risorse che supportano le funzioni e i processi aziendali critici.

Classificazione delle funzioni, dei processi e delle risorse

3.3 I prestatori di servizi di pagamento dovrebbero classificare sotto il profilo della criticità le funzioni aziendali, i processi di supporto e le risorse informatiche individuate.

Valutazioni dei rischi delle funzioni, dei processi e delle risorse

3.4 I prestatori di servizi di pagamento dovrebbero garantire il monitoraggio continuo delle minacce e delle vulnerabilità, nonché rivedere periodicamente gli scenari di rischio che hanno impatti sulle funzioni aziendali, i processi critici e le risorse informatiche. In quanto parte dell'obbligo di condurre e fornire alle autorità competenti una valutazione aggiornata e approfondita dei rischi operativi e di sicurezza relativi ai servizi di pagamento che prestano e dell'adeguatezza delle misure di mitigazione e dei meccanismi di controllo messi in atto per affrontarli - come previsto dall'articolo 95, paragrafo 2, della direttiva (UE) 2015/2366 - i prestatori di servizi di pagamento dovrebbero eseguire e documentare, almeno su base annua, o a intervalli più ravvicinati determinati dall'autorità competente, valutazioni dei rischi delle funzioni, dei processi e delle risorse informatiche che hanno individuato e classificato come rilevanti ai fini dei principali rischi operativi e di sicurezza. Tali valutazioni dei rischi dovrebbero essere eseguite anche prima che sia attuata qualsiasi modifica sostanziale delle infrastrutture, dei processi o delle procedure tale da pregiudicare la sicurezza dei servizi di pagamento.

3.5 Sulla base delle valutazioni dei rischi, i prestatori di servizi di pagamento dovrebbero stabilire se e in quale misura sia necessario modificare le misure di sicurezza esistenti, le tecnologie utilizzate e le procedure o i servizi di pagamento offerti. I prestatori di servizi di pagamento dovrebbero tenere conto del tempo necessario per mettere in pratica le modifiche e del tempo necessario per adottare adeguate misure di sicurezza provvisorie per ridurre al minimo gli incidenti operativi o di sicurezza, le frodi e potenziali impatti dirompenti per la prestazione dei servizi di pagamento.

Orientamento 4: Protezione

4.1 I prestatori di servizi di pagamento dovrebbero definire e attuare misure di sicurezza preventive per contrastare i rischi operativi e di sicurezza individuati. Tali misure dovrebbero garantire un adeguato livello di sicurezza sulla base dei rischi individuati.

4.2 I prestatori di servizi di pagamento dovrebbero definire e attuare un approccio di «difesa in profondità», stabilendo controlli su più livelli nei confronti delle persone, dei processi e della tecnologia, in cui ogni livello agisce da rete di sicurezza per i livelli precedenti. La difesa in profondità dovrebbe intendersi come la realizzazione di più di un controllo a presidio dello stesso rischio, ad esempio attraverso l'applicazione del principio del doppio controllo, l'autenticazione a due fattori, la segmentazione della rete ed i firewall multipli.

4.3 I prestatori di servizi di pagamento dovrebbero garantire la riservatezza, l'integrità e la disponibilità delle loro risorse logiche e fisiche critiche, e dei dati sensibili per i servizi di pagamento relativi ai loro utenti, sia che essi siano inutilizzati, in transito o in uso. Se i dati comprendono dati personali, tali misure dovrebbero essere attuate conformemente al regolamento (UE) 2016/679[6] o, se applicabile, al regolamento (CE) n. 45/2001[7].

[6] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

4.4 I prestatori di servizi di pagamento dovrebbero stabilire, su base continuativa, se modifiche al contesto operativo esistente possano influenzare le misure di sicurezza adottate o se si renda necessaria l'adozione di ulteriori misure per mitigare il rischio collegato. Tali modifiche dovrebbero essere formalmente parte del processo per la gestione del cambiamento adottato dal prestatore di servizi di pagamento, processo che dovrebbe garantire che le modifiche siano adeguatamente pianificate, verificate, documentate e autorizzate. In base alle minacce di sicurezza osservate e alle modifiche realizzate, si dovrebbero condurre verifiche per considerare scenari di attacchi potenziali rilevanti e noti.

4.5 Nel progettare, sviluppare e fornire servizi di pagamento, i prestatori di servizi di pagamento dovrebbero garantire l'applicazione dei principi di segregazione dei compiti e di «minimo privilegio». I prestatori di servizi di pagamento dovrebbero particolare attenzione alla separazione degli ambienti IT, in particolare di sviluppo, collaudo e produzione.

Integrità e riservatezza dei dati e dei sistemi

4.6 I prestatori di servizi di pagamento dovrebbero garantire che durante la progettazione, lo sviluppo e la prestazione dei servizi, le attività di raccolta, instradamento, trattamento, memorizzazione e/o archiviazione nonché di visualizzazione dei dati sensibili per i servizi di pagamento degli utenti siano adeguate, pertinenti e limitate a quanto strettamente necessario per la prestazione dei servizi stessi.

4.7 I prestatori di servizi di pagamento dovrebbero accertarsi periodicamente che il software utilizzato per la prestazione dei loro servizi, compreso quello utilizzato dagli utenti relativo ai pagamenti, sia aggiornato e che siano applicate le *patch* critiche per la sicurezza. I prestatori di servizi di pagamento dovrebbero garantire che sui loro servizi di pagamento siano operanti meccanismi di controllo dell'integrità del software, del firmware e delle informazioni.

Sicurezza fisica

4.8 I prestatori di servizi di pagamento dovrebbero disporre di adeguate misure di sicurezza fisica, in particolare per proteggere i dati sensibili per i servizi di pagamento degli utenti ed i sistemi ICT utilizzati per fornire tali servizi.

Controllo dell'accesso

4.9 L'accesso fisico e logico ai sistemi ICT dovrebbe essere permesso soltanto a persone autorizzate. L'autorizzazione dovrebbe essere rilasciata tenendo conto dei compiti e delle responsabilità dei dipendenti e soltanto alle persone adeguatamente addestrate e controllate. I prestatori di servizi di pagamento dovrebbero istituire controlli per limitare in modo affidabile l'accesso ai sistemi ICT

[7] Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).

solo alle persone in possesso di un legittimo requisito aziendale. L'accesso ai dati e ai sistemi per mezzo di applicazioni informatiche dovrebbe essere limitato a quanto strettamente necessario per la prestazione del servizio in questione.

4.10 I prestatori di servizi di pagamento dovrebbero controllare rigidamente l'accesso privilegiato al sistema limitando strettamente e sorvegliando attentamente i dipendenti in possesso di ampie autorizzazioni di accesso. Dovrebbero essere eseguiti controlli quali l'accesso basato sulle funzioni, la registrazione e la revisione delle attività dei sistemi degli utenti privilegiati, l'autenticazione forte e il monitoraggio delle anomalie. I prestatori di servizi di pagamento dovrebbero gestire i diritti di accesso alle risorse informatiche e ai loro sistemi di supporto sulla base delle esigenze conoscitive contingenti. I diritti di accesso dovrebbero essere sottoposti a revisioni periodiche.

4.11 Dovrebbero essere tenuti registri degli accessi per un periodo commisurato al livello di criticità delle funzioni aziendali, dei processi di supporto e delle risorse informatiche, conformemente agli orientamenti 3.1 e 3.2, fatti salvi gli obblighi di conservazione previsti dalla normativa nazionale e dell'UE. I prestatori di servizi di pagamento dovrebbero utilizzare questi registri per facilitare l'individuazione di attività anomale per la prestazione dei servizi di pagamento, nonché le relative indagini.

4.12 Al fine di garantire la sicurezza delle comunicazioni e ridurre il rischio, l'accesso amministrativo da remoto a componenti critiche dei sistemi ICT dovrebbe essere concesso esclusivamente sulla base delle esigenze conoscitive contingenti e qualora siano applicate soluzioni di autenticazione forte.

4.13 Il funzionamento di prodotti, strumenti e procedure relativi ai processi di controllo degli accessi dovrebbe garantire che lo stesso processo di controllo non sia compromesso o eluso. Ciò vale anche per la sottoscrizione, la consegna, la revoca e il ritiro dei corrispondenti prodotti, strumenti e procedure.

Orientamento 5: Rilevazione delle violazioni di sicurezza

Monitoraggio nel continuo e rilevazione delle violazioni di sicurezza

5.1 I prestatori di servizi di pagamento dovrebbero stabilire e applicare processi e capacità per il monitoraggio nel continuo delle funzioni aziendali, dei processi di supporto e delle risorse informatiche, al fine di rilevare attività anomale nella prestazione dei servizi di pagamento. Nell'ambito di questo monitoraggio, i prestatori di servizi di pagamento dovrebbero disporre di capacità adeguate ed efficaci per rilevare intrusioni fisiche o logiche e violazioni della riservatezza, dell'integrità e della disponibilità delle risorse informatiche utilizzate nella prestazione dei servizi di pagamento.

5.2 I processi di monitoraggio nel continuo e la rilevazione delle violazioni di sicurezza dovrebbero riguardare:

a) i fattori interni ed esterni importanti, comprese le funzioni di gestione del business e dell'ICT aziendali;

b) le transazioni, al fine di individuare eventuali abusi negli accessi da parte dei fornitori o di altri soggetti;

c) potenziali minacce interne ed esterne.

5.3 I prestatori di servizi di pagamento dovrebbero realizzare misure per identificare: possibili fughe di informazioni, codici nocivi (malware) e altre minacce per la sicurezza, nonché vulnerabilità conosciute pubblicamente del proprio software e hardware ed i corrispondenti aggiornamenti dei controlli di sicurezza.

Monitoraggio e segnalazione di incidenti operativi o di sicurezza

5.4 I prestatori di servizi di pagamento dovrebbero definire criteri e soglie appropriati per la classificazione di un evento come incidente operativo o di sicurezza, conformemente a quanto previsto nella sezione «Definizioni» dei presenti orientamenti, nonché indicatori di preallerta che consentano l'individuazione rapida di incidenti operativi o di sicurezza.

5.5 I prestatori di servizi di pagamento dovrebbero definire processi e strutture organizzative appropriati per garantire il coerente e integrato monitoraggio, la gestione, e il *follow-up* degli incidenti operativi o di sicurezza.

5.6 I prestatori di servizi di pagamento dovrebbero definire una procedura per la segnalazione all'alta dirigenza degli incidenti operativi o di sicurezza e dei reclami dei clienti in materia di sicurezza.

Orientamento 6: Continuità operativa

6.1 I prestatori di servizi di pagamento dovrebbero impiantare una solida gestione della continuità operativa allo scopo di massimizzare la propria capacità di prestare servizi di pagamento su base continuativa e per limitare le perdite in caso di gravi interruzioni dell'operatività.

6.2 Al fine di impiantare una solida gestione della continuità operativa, i prestatori di servizi di pagamento dovrebbero attentamente analizzare la propria esposizione a gravi interruzioni dell'operatività e valutare, dal punto di vista quantitativo e qualitativo, le possibili ripercussioni di tali eventi, ricorrendo ad analisi interne e/o esterne dei dati e degli scenari. Sulla base delle funzioni, dei processi, dei sistemi, delle operazioni e delle interdipendenze individuati e classificati come critici, in accordo con gli orientamenti da 3.1 a 3.3, i prestatori di servizi di pagamento dovrebbero attribuire priorità alle azioni da svolgere per la continuità operativa ricorrendo ad un approccio basato sul rischio, che può utilizzare allo scopo le valutazioni dei rischi compiute ai sensi dell'orientamento 3. A seconda del modello di business del singolo prestatore di servizi di pagamento ciò consente, ad esempio, di facilitare l'ulteriore trattamento di operazioni critiche mentre proseguono gli interventi di ripristino.

6.3 Sulla base delle analisi eseguite ai sensi dell'orientamento 6.2, il prestatore di servizi di pagamento dovrebbe realizzare:

a) piani per la continuità operativa in grado di garantire che esso reagisca appropriatamente alle emergenze e sia capace di mantenere operative le proprie attività aziendali critiche;

b) misure di mitigazione da adottare in caso di interruzione dei propri servizi di pagamento e di cessazione dei contratti vigenti, al fine di evitare effetti negativi sui sistemi di pagamento e sugli utenti dei servizi, nonché per garantire l'esecuzione delle operazioni di pagamento in corso.

Pianificazione della continuità operativa basata sugli scenari

6.4 I prestatori di servizi di pagamento dovrebbero considerare una gamma di diversi scenari, ivi compresi quelli estremi purché plausibili, ai quali potrebbero essere esposti, e valutarne gli impatti potenziali.

6.5 Sulla base delle analisi eseguite ai sensi dell'orientamento 6.2 e degli scenari plausibili individuati ai sensi dell'orientamento 6.4, i prestatori di servizi di pagamento dovrebbero elaborare piani di risposta e ripristino che dovrebbero:

a) concentrarsi sugli impatti operativi delle funzioni, dei processi, dei sistemi, delle transazioni e delle interdipendenze critici;

b) essere documentati e messi a disposizione delle unità aziendali e di supporto, nonché prontamente accessibili in caso di emergenza;

c) essere aggiornati sulla base di quanto appreso dalle verifiche, dall'individuazione di nuovi rischi e minacce, nonché dai cambiamenti degli obiettivi e dalle priorità di ripristino.

Verifica dei piani di continuità operativa

6.6 I prestatori di servizi di pagamento dovrebbero sottoporre a verifica i propri piani per la continuità operativa e garantire che almeno annualmente siano effettuate verifiche su funzioni, processi e sistemi, transazioni e interdipendenze critici. I piani dovrebbero supportare gli obiettivi di proteggere e, se necessario, ripristinare l'integrità e la disponibilità delle operazioni, nonché la riservatezza delle risorse informatiche.

6.7 I piani dovrebbero essere aggiornati almeno a cadenza annuale sulla base dei risultati delle verifiche, delle informazioni sulle minacce correnti, della condivisione delle informazioni e degli insegnamenti appresi grazie a eventi precedenti, dei mutevoli obiettivi di ripristino e delle analisi degli scenari operativamente e tecnicamente plausibili non ancora verificatisi, nonché, se del caso, dopo modifiche dei sistemi e dei processi. In sede di definizione delle migliori prassi correnti, i prestatori di servizi di pagamento dovrebbero consultare e coordinarsi con le rilevanti parti interessate interne ed esterne.

6.8 Le verifiche da parte dei prestatori di servizi di pagamento dei loro piani per la continuità operativa dovrebbero:

a) comprendere una gamma adeguata di scenari, come indicato nell'orientamento 6.4;

b) essere progettate in modo tale da mettere alla prova le ipotesi su cui i piani per la continuità operativa si fondano, inclusi le disposizioni organizzative e i piani di comunicazione in caso di crisi;

c) includere le procedure per verificare la capacità del personale e dei processi aziendali di reagire adeguatamente agli scenari su indicati.

6.9 I prestatori di servizi di pagamento dovrebbero monitorare periodicamente l'efficacia dei loro piani per la continuità operativa, nonché documentare e analizzare eventuali difficoltà o fallimenti risultanti dalle verifiche.

Comunicazione in caso di crisi

6.10 In caso di interruzione del business, o emergenza, e durante l'esecuzione dei piani per la continuità operativa, i prestatori di servizi di pagamento dovrebbero disporre di efficaci misure per la comunicazione in caso di crisi, tali da garantire un'informativa tempestiva e appropriata a tutte le parti interessate rilevanti, interne ed esterne, compresi i fornitori di servizi esterni.

Orientamento 7: Verifica delle misure di sicurezza

7.1 I prestatori di servizi di pagamento dovrebbero istituire e realizzare un quadro di riferimento per la verifica delle misure di sicurezza che convalidi la solidità e l'efficacia di queste misure, nonché garantire che tale quadro di riferimento consideri le nuove minacce e vulnerabilità individuate grazie alle attività di monitoraggio dei rischi.

7.2 I prestatori di servizi di pagamento dovrebbero garantire l'esecuzione di verifiche in caso di modifica delle infrastrutture, dei processi o delle procedure, nonché in caso di modifiche apportate a seguito di gravi incidenti operativi o di sicurezza.

7.3 Il quadro di riferimento per la verifica delle misure di sicurezza dovrebbe comprendere anche le misure rilevanti per i) i terminali ed i dispositivi utilizzati per la prestazione dei servizi di pagamento, ii) i terminali ed i dispositivi utilizzati per l'autenticazione degli utenti dei servizi di pagamento e iii) i dispositivi ed il software forniti dai prestatori di servizi di pagamento agli utenti per generare/ricevere un codice di autenticazione.

7.4 Il quadro di riferimento per la verifica delle misure di sicurezza dovrebbe garantire che:

a) al fine di assicurare la solidità e l'efficacia delle misure di sicurezza, le verifiche siano eseguite nell'ambito del processo formale di gestione del cambiamento adottato dal prestatore di servizi di pagamento;

b) le verifiche siano eseguite da revisori indipendenti, in possesso di sufficienti conoscenze, abilità e competenze in materia di verifica delle misure di sicurezza dei servizi di

pagamento, e non coinvolti nello sviluppo delle misure di sicurezza dei servizi o sistemi di pagamento oggetto delle verifiche stesse, quanto meno nel caso delle verifiche finali eseguite prima della messa in opera delle misure di sicurezza;

c) le verifiche del prestatore dei servizi di pagamento comprendano scansioni della vulnerabilità (vulnerability scan) e prove di penetrazione (penetration test) adeguate al livello di rischio individuato per i servizi di pagamento.

7.5 I prestatori di servizi di pagamento dovrebbero eseguire verifiche continuative e ripetute delle misure di sicurezza per i loro servizi. Nel caso di sistemi critici per la prestazione dei servizi di pagamento (come identificati nell'orientamento 3.2), le verifiche dovrebbero essere eseguite almeno annualmente. Per i sistemi non critici le verifiche dovrebbero essere periodiche, secondo un approccio basato sul rischio, e comunque almeno ogni tre anni.

7.6 I prestatori di servizi di pagamento dovrebbero monitorare e valutare i risultati ottenuti dalle verifiche delle misure di sicurezza e di conseguenza aggiornare quelle d'interesse e, nel caso dei sistemi critici, senza indebiti ritardi.

Orientamento 8: Consapevolezza della situazione e apprendimento continuo

Panorama delle minacce e consapevolezza della situazione

8.1 I prestatori di servizi di pagamento dovrebbero definire e impiantare processi e strutture organizzative per l'individuazione ed il monitoraggio continuo delle minacce alla sicurezza e all'operatività che potrebbero pregiudicare in modo sostanziale la loro capacità di prestare servizi di pagamento.

8.2 I prestatori di servizi di pagamento dovrebbero analizzare gli incidenti operativi o di sicurezza che sono stati individuati o si sono verificati all'interno e/o all'esterno dell'ente. I prestatori di servizi di pagamento dovrebbero considerare quanto appreso da tali analisi e aggiornare di conseguenza le proprie misure di sicurezza.

8.3 I prestatori di servizi di pagamento dovrebbero monitorare attivamente gli sviluppi tecnologici per garantire di essere aggiornati sui rischi per la sicurezza.

Programmi di formazione e di sensibilizzazione in tema di sicurezza

8.4 I prestatori di servizi di pagamento dovrebbero definire un programma di formazione destinato a tutti i propri dipendenti per garantire che essi siano preparati ad adempiere i compiti e le responsabilità loro assegnati conformemente alle prassi e procedure di sicurezza dell'azienda, con lo scopo di ridurre gli errori umani, i furti, le frodi, gli abusi o le perdite. I prestatori di servizi di pagamento dovrebbero garantire che il programma di formazione offra ai loro dipendenti occasioni formative in materia di sicurezza almeno a cadenza annuale o, se necessario, con maggiore frequenza.

8.5 I prestatori di servizi di pagamento dovrebbero garantire che coloro che occupano in azienda i posti chiave identificati nell'orientamento 3.1, ricevano una formazione mirata sulla sicurezza delle informazioni a cadenza annuale o, se necessario, con maggiore frequenza.

8.6 I prestatori di servizi di pagamento dovrebbero definire e attuare programmi periodici di sensibilizzazione alla sicurezza al fine di educare i propri dipendenti e affrontare i rischi relativi alla sicurezza informatica. Questi programmi dovrebbero prescrivere ai dipendenti dei prestatori di servizi di pagamento di segnalare qualsiasi attività insolita ed eventuali incidenti.

Orientamento 9: Gestione del rapporto con gli utenti dei servizi di pagamento

Conoscenza da parte degli utenti dei servizi di pagamento dei rischi per la sicurezza e delle azioni di mitigazione del rischio

9.1 I prestatori di servizi di pagamento dovrebbero definire e attuare processi per accrescere le conoscenze da parte degli utenti dei servizi di pagamento dei rischi per la sicurezza connessi ai servizi stessi, fornendo agli utenti assistenza e orientamento.

9.2 L'assistenza e l'orientamento forniti agli utenti dei servizi di pagamento dovrebbero essere aggiornati in relazione alle nuove minacce e vulnerabilità; gli aggiornamenti dovrebbero essere comunicati agli utenti.

9.3 Laddove permesso dalle modalità di funzionamento del servizio, i prestatori di servizi di pagamento dovrebbero consentire agli utenti di disattivare specifiche funzioni di pagamento connesse ai servizi di pagamento offerti.

9.4 Qualora, ai sensi dell'articolo 68, paragrafo 1, della direttiva (UE) 2015/2366, un prestatore di servizi di pagamento abbia concordato con il pagatore limiti di spesa per le operazioni di pagamento eseguite mediante strumenti di pagamento specifici, il prestatore dovrebbe concedere al pagatore la possibilità di modificare tali limiti elevandoli al limite massimo concordato.

9.5 I prestatori di servizi di pagamento dovrebbero offrire agli utenti la possibilità di ricevere avvisi in caso di tentativi, iniziati e/o falliti, di effettuare operazioni di pagamento, consentendo così agli utenti di rilevare un uso fraudolento o dannoso del proprio conto.

9.6 I prestatori di servizi di pagamento dovrebbero tenere gli utenti al corrente degli aggiornamenti delle procedure di sicurezza che li riguardano per la prestazione dei servizi di pagamento.

9.7 I prestatori di servizi di pagamento dovrebbero fornire agli utenti assistenza su tutte le domande, le richieste di aiuto e le notifiche di anomalie o le questioni riguardanti la sicurezza dei servizi di pagamento. Gli utenti dei servizi di pagamento dovrebbero essere adeguatamente informati su come ottenere tale assistenza.