walderwyss studio legale

Walder Wyss SA
Seefeldstrasse 123
Casella postale
8034 Zurigo
Svizzera

Telefono +41 58 658 58 58
Fax +41 58 658 59 59
www.walderwyss.com

Sommario esecutivo

a	Istituto nazionale di test per la cibersicurezza (NTC)
da	Michael Isler, Oliver Kunz, Gina Moll
oggetto	**Responsabilità penale dell'hacking etico**
data	26 giugno 2023

Michael Isler
Partner
Dr. iur.
Avvocato
Diretto +41 58 658 55 15
michael.isler@walderwyss.com

Oliver Kunz
Partner
lic. iur., LL.M.
Avvocato
Diretto +41 58 658 56 41
oliver.kunz@walderwyss.com

Gina Moll
Associate
M.A. HSG in Law, LL.M.
Avvocato
Diretto +41 58 658 51 56
gina.moll@walderwyss.com

1. Sommario esecutivo

1.1. Fattispecie e incarico agli esperti

1 L'Istituto nazionale di test per la cibersicurezza NTC nell'ambito del programma di analisi delle falle di sicurezza testa i prodotti digitali e le infrastrutture di rete (sistemi). Le analisi vengono in parte eseguite come progetti commissionati con il relativo consenso degli operatori di sistema, in parte come cosiddetti progetti di iniziativa, ossia su iniziativa dell'istituto stesso, senza un consenso preventivo. Nell'ambito dei progetti di iniziativa, l'NTC testa i prodotti e le infrastrutture digitali non testati o testati in modo insufficiente. In questo modo, l'NTC mira ad aumentare la cibersicurezza nell'interesse degli utenti dei sistemi e del pubblico in generale.

2 In quanto organizzazione senza scopo di lucro finanziata con fondi pubblici, l'NTC non persegue interessi finanziari o scopi di profilazione. Nello specifico, l'NTC si concentra su sistemi socialmente rilevanti (in particolare sistemi diffusi, critici, senza alternative e governativi che appaiono a rischio sulla base di indicazioni oggettive, ad esempio perché vi sono indicazioni di lacune nella sicurezza di un sistema target.

3 Nel condurre le valutazioni sulle falle di sicurezza, l'NTC aderisce alle regole di best practice del Centro nazionale per la cibersicurezza NCSC.

4 Sulla base della sua *politica di divulgazione delle vulnerabilità*, l'NTC intende comunicare i risultati dei progetti di iniziativa in modo appropriato ai produttori e agli operatori dei sistemi target e, in una fase successiva, pubblicarli in forma

appropriata affinché la società, la popolazione, le autorità e la scienza possano trarne beneficio.

5 A causa della concezione dei progetti di iniziativa come progetti senza contratto sorgono diversi interrogativi in merito alla possibile responsabilità penale ai sensi del diritto penale ("ciber") svizzero.

1.2. Responsabilità penale ai sensi dell'art. 143bis CPS e dell'art. 144bis cpv. 1 CPS

6 L'esecuzione dell'analisi delle falle di sicurezza - nella misura in cui comportano la penetrazione (tentata o effettiva) di un sistema di elaborazione dati altrui (test di penetrazione) - è potenzialmente in conflitto con il reato di hacking ai sensi dell'art. 143bis cpv. 1 CPS. Ai sensi del quale, è punibile "chiunque si introduce indebitamente, per mezzo di un dispositivo di trasmissione dei dati, in un sistema altrui per l'elaborazione di dati specialmente protetto contro ogni suo accesso è punito, a querela di parte, con una pena detentiva sino a tre anni o con una pena pecuniaria". La motivazione dell'atto penalmente rilevante è irrilevante ai fini della definizione del reato. La fattispecie mira in generale a proteggere i sistemi di elaborazione dati dall'accesso non autorizzato. Il bene giuridico tutelato in questo caso è la "pace informatica", ovvero la libertà della persona autorizzata di decidere a chi concedere l'accesso al proprio sistema di elaborazione dati protetto e ai dati in esso contenuti.

7 Poiché nel caso dei progetti di iniziativa, tra l'altro, vengono effettuati tentativi mirati tramite test di penetrazione per indagare eventuali lacune nel sistema di sicurezza di un sistema target senza il consenso dei portatori del bene giuridico protetto e quindi senza autorizzazione, sussiste il rischio di responsabilità penale. Il tentativo di intrusione è punibile anche quando viene superata l'area degli atti preparatori non punibili (come la ricognizione di un potenziale sistema bersaglio tramite *portscan*).

8 La pubblicazione dei risultati dei progetti di iniziativa non è problematica ai sensi dell'art. 143bis cpv. 2 CPS (che criminalizza la fornitura di dati che possono essere utilizzati per commettere un reato ai sensi dell'art. 143bis cpv. 1 CP), a condizione che la vulnerabilità di sicurezza pubblicata sia già stata completamente eliminata prima della pubblicazione. Un approccio temporalmente coordinato con l'operatore del sistema target interessato può quindi escludere completamente la responsabilità penale ai sensi dell'art. 143bis cpv. 2 CPS. Tuttavia, se la vulnerabilità di sicurezza creata da una lacuna di sicurezza non è ancora (o non è completamente) chiusa prima della pubblicazione dei dettagli tecnici, il rischio penale può essere minimizzato solo con un livello di dettaglio inferiore nella pubblicazione. In questi casi, non dovrebbero essere pubblicati dettagli concreti di un possibile *exploit* e la descrizione tecnica della falla di sicurezza dovrebbe essere limitata alle

informazioni necessarie per consentire agli utenti interessati di adottare misure di protezione adeguate. In questi casi, la segnalazione a un'autorità, come l'NCSC, non porrebbe problemi ai sensi dell'articolo 143bis cpv. 2 CPS.

9 In considerazione della possibile responsabilità penale per il danneggiamento dei dati ai sensi dell'art. 144bis n.1 CPS, le manipolazioni temporanee dei dati (ad esempio per superare una barriera di sicurezza) dovrebbero essere eseguite solo con la minore intensità di intervento possibile e per la durata più breve possibile, poiché in caso contrario si dovrebbe affermare la materialità dell'alterazione dei dati ai sensi del reato (ad esempio, le password temporaneamente modificate o simili devono essere immediatamente ripristinate). Esiste anche un rischio aggiuntivo ai sensi del diritto penale per quanto riguarda un'eventuale commissione intenzionale dell'art. 144bis n.1 CPS, ad esempio se un'azione tecnicamente rischiosa viene intrapresa con la consapevolezza che potrebbe portare a un danno ai dati (ad esempio, la temporanea o permanente indisponibilità dei dati). La responsabilità penale ai sensi dell'art. 144bis n.2 CPS (diffusione di programmi che danneggiano i dati), invece, può essere esclusa nel contesto di progetti di iniziativa.

1.3. Stato di necessità esimente ai sensi dell'art. 17 CPS

10 Un comportamento che soddisfa gli elementi di un reato può, in circostanze particolari, eccezionalmente non essere illegale e quindi esente da pena. Ciò è particolarmente vero se la persona che agisce in conformità con il reato può invocare la giustificazione penale della necessità esimente ai sensi dell'art. 17 CPS.

11 Si considera commesso un atto di necessità se l'atto in questione è stato compiuto per salvare i propri interessi legali o quelli di terzi da un pericolo immediato che non poteva essere evitato in altro modo. L'azione (che in linea di principio è punibile) è eccezionalmente lecita se la persona autorizzata ad agire in stato di necessità esimente protegge interessi di valore superiore.

12 I presupposti concreti dello stato di necessità esimente sono l'esistenza di (i) un pericolo immediato per un bene giuridico individuale (ad esempio, il diritto individuale alla libertà di "pace informatica"), (ii) l'assoluta sussidiarietà (cioè, l'atto deve rappresentare il mezzo più blando possibile per scongiurare il pericolo) e (iii) una ponderazione positiva degli interessi. Da un punto di vista soggettivo, è necessario che (iv) la persona autorizzata ad agire in uno stato di necessità esimente sia consapevole della situazione di necessità e agisca per salvare il bene giuridico minacciato.

13 Se un test di penetrazione viene effettuato per scongiurare una minaccia all'integrità e alla sicurezza del sistema corrispondente (in particolare perché vi sono indicazioni concrete che il sistema è affetto da potenziali vulnerabilità di

sicurezza che consentono anche interventi malevoli), il sistema interessato è potenzialmente vulnerabile agli attacchi in qualsiasi momento. In queste condizioni, il pericolo imminente per un bene giuridico individuale (ovvero la "pace informatica" dei titolari dei beni giuridici colpiti) necessario per invocare lo stato di necessità esimente esiste in linea di principio. L'immediatezza del pericolo deriva, nel caso di apparecchiature/sistemi di elaborazione dati in pericolo, dalla condizione di minaccia per un periodo di tempo più lungo, che può trasformarsi in un danno (ad es. attacco di un hacker malintenzionato, danneggiamento dei dati, perdita di dati, ecc.)

14 In uno stato di necessità esimente, i mezzi utilizzati devono essere idonei a scongiurare il pericolo, e devono anche essere i più blandi, cioè quelli meno lesivi dei beni giuridici altrui (sussidiarietà assoluta).

15 I progetti di iniziativa sono conformi al principio di sussidiarietà assoluta se l'intervento si limita a scoprire le falle di sicurezza di sicurezza esistenti, a documentarle e a divulgarle successivamente agli operatori dei sistemi target affinché possano porre rimedio allo stato di pericolo. Inoltre, deve essere impossibile o irragionevole ottenere il consenso preventivo di tutti i potenziali titolari del bene giuridico. Ciò è particolarmente vero se si stanno testando sistemi target in cui non è possibile identificare in modo definitivo tutti i titolari del bene giuridico potenzialmente interessati o che possono e vogliono reagire in modo adeguato. Talvolta, il contatto preventivo (e la relativa divulgazione della falla di sicurezza) potrebbe addirittura aumentare il rischio che la falla di sicurezza venga sfruttata.

16 Alle suddette condizioni, anche il bilanciamento degli interessi nei progetti d'iniziativa è positivo: la gravità dell'accesso (controllato) con uno scopo positivo (e senza l'intenzione di arrecare danno) nel contesto di un progetto d'iniziativa è chiaramente secondaria rispetto al grado significativamente più elevato di pericolo per lo stesso interesse legale nel caso di un attacco di hacker malintenzionati.

17 Ciò che è rilevante, tuttavia, è che i progetti di iniziativa siano realizzati esclusivamente allo scopo di eliminare il pericolo. Se si perseguono altri scopi (ad esempio l'autoprofilazione, la curiosità o anche l'ottenimento di vantaggi economici), un hacker non potrà invocare la giustificazione dello stato di necessità. In definitiva, la giustificazione della necessità ai sensi dell'art. 17 CPS è idonea a giustificare qualsiasi azione ai sensi dell'art. 143bis cpv. 1 del CPS e dell'articolo 144bis n.1 del CPS nell'ambito dell'attuazione dei progetti di iniziativa dell'NTC.

1.4. Ulteriori rischi ai sensi del diritto penale

18 Per quanto riguarda gli altri reati previsti dal diritto penale in materia di cibersicurezza (in particolare l'art. 179novies CPS [acquisizione non autorizzata di dati personali] e l'art. 45c LTC c.d. l'art. 53 LTC [violazione della Legge sulle telecomunicazioni], il reato può già essere evitato grazie a una pianificazione adeguata dei progetti d'iniziativa e alla corrispondente realizzazione delle analisi delle falle di sicurezza. Qualora il reato si realizzi in casi eccezionali, lo stato di necessità esimente può essere utilizzato come giustificazione alle condizioni previste.