Numero			Bellinzona
1084	cl	0	9 marzo 2022

Consiglio di Stato
Piazza Governo 6
Casella postale 2170
6501 Bellinzona
telefono +41 91 814 41 11
fax +41 91 814 44 35
e-mail can@ti.ch
web www.ti.ch

Repubblica e Cantone
Ticino

Il Consiglio di Stato

Dipartimento federale dell'ambiente, dei trasporti e delle comunicazioni DATEC
Palazzo federale
3003 Berna

tp-secretariat@bakom.admin.ch

Procedura di consultazione - Modifica dell'ordinanza sui servizi di telecomunicazione (sicurezza delle informazioni, delle infrastrutture e dei servizi di telecomunicazione)

Gentili signore, egregi signori,

la ringraziamo per averci consultato in merito alla modifica dell'ordinanza in oggetto, sulla quale esprimiamo volentieri le seguenti osservazioni.

Lo scrivente Consiglio sostiene il progetto di modifica dell'ordinanza sui servizi di telecomunicazione (OST) presentato; esso mira a combattere la manipolazione non autorizzata delle apparecchiature di telecomunicazione ed è in linea con quanto discusso negli ultimi anni a livello di sicurezza e di "Enterprise Incident Response", dove il peso è passato dal credere di poter proteggere perfettamente un'infrastruttura al gestire eventuali attacchi e conseguenze in aggiunta ad una protezione standardizzata. Oggi la protezione delle infrastrutture informatiche fa parte del "business model" di ogni azienda e i metodi di protezione sono standardizzati e basati su linee guida internazionali. Tipicamente la protezione è assicurata al 90-95% (a dipendenza del budget) lasciando un 5-10% di probabilità d'avere degli attacchi chiamati "zero day", ovvero sconosciuti fino al momento dell'utilizzo.
In particolare, riteniamo che sia urgente e necessario attuare ed estendere le misure per raggiungere un livello minimo di sicurezza anche per la rete 5G (e successive) in Svizzera.
A tal proposito segnaliamo alcuni ambiti, legati prevalentemente alle attività della difesa, della sicurezza, degli interventi di soccorso e della protezione di infrastrutture strategiche, nei quali i principi contenuti nella modifica in oggetto andrebbero estesi.

Oggi, più del 70% delle chiamate d'emergenza sono effettuate tramite telefoni cellulari; di conseguenza, le interruzioni della rete di telefonia mobile hanno conseguenze significative. Hanno implicazioni dirette per le chiamate di emergenza e per il controllo degli eventi da parte delle organizzazioni a tutela della sicurezza e di soccorso, così come per gli operatori di infrastrutture critiche, che devono poter contare su reti di telefonia mobile affidabili e sicure allo stato dell'arte.

Le organizzazioni legate alla sicurezza ed al soccorso e le infrastrutture critiche vanno di conseguenza integrate maggiormente nei processi di allarme e notifica.

Gli attacchi informatici non solo hanno un forte impatto economico, ma mettono anche in pericolo la sicurezza del paese, in quanto possono portare a guasti o malfunzionamenti delle infrastrutture critiche e/o sensibili. Per questo motivo, i fornitori di servizi Internet devono poter bloccare queste e altre risorse di indirizzamento che rappresentano una minaccia per le infrastrutture di cui sopra. Questo aspetto è regolato dall'art. 96 cpv. 3 ma va maggiormente sviluppato in funzione della criticità e della sensibilità dell'obbiettivo colpito. L'introduzione di un obbligo di bloccare selettivamente l'accesso a Internet e alle risorse di indirizzamento che rappresentano una minaccia per le infrastrutture critiche/strategiche è auspicato.
A complemento di quanto sopra si impone però una riflessione affinché le misure citate non collidano con le prescrizioni inerenti alla sfera privata degli utenti "comuni". Se per un'azienda è plausibile il controllo delle transazioni da e per la rete interna questo è meno praticabile su vasta scala e in relazione a piccole realtà domestiche dove una certa privacy e libertà sono auspicabili (es: sfera sessuale, medica, libertà di espressione o religiosa).
Una selezione si impone in funzione della criticità della minaccia e dell'obbiettivo colpito:

1) Per esempio si potrebbero esplicitamente quantificare il minimo di banda da cui iniziare questi "blocchi". Questo eviterebbe che un privato che si trova vittima di un malware e che genera traffico malevolo ma di entità limitata dal proprio abbonamento di casa, si trovi il proprio traffico analizzato in qualche ufficio del fornitore di servizi in modo mirato.

2) Alternativamente si potrebbe anche specificare che i blocchi dovrebbero esser frutto di analisi aggregate e anonimizzate (con prova del rispetto della privacy), dove la decisione sia basata su un tipico grafico gravità/estensione e quindi ponderato secondo il reale rischio che un attacco porta, salvaguardando comunque la possibilità di intervenire in modo più deciso ed incisivo qualora si verifichino attacchi miranti a colpire obbiettivi critici ed a valenza strategica.

Per migliorare il trattamento e la diffusione delle segnalazioni di perturbazioni che si ricevono, la revisione dell'ordinanza in consultazione prevede un ruolo rafforzato della Centrale nazionale d'allarme (CE-NAL), che gestisce 24 ore su 24 un'infrastruttura informatica sicura (art. 96). D'altra parte, gli attacchi informatici devono essere segnalati a un servizio di segnalazione (art. 96b) che deve ancora essere istituito. Inoltre, ci sono altre organizzazioni che si occupano di attacchi informatici. Per esempio, la Centrale nazionale di sicurezza informatica (CNSC), la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) e le centrali d'allarme cantonali devono essere incluse nelle attività. Per questo motivo, non è possibile che l'UFCOM sia il solo ad essere informato dalla CENAL sulle segnalazioni di interferenze ricevute. I ruoli di tutti i servizi all'interno del processo globale di segnalazione e di allarme nel dominio cibernetico devono essere presentati in dettaglio nel rapporto esplicativo. La creazione di un unico punto di contatto (SPOC) dovrebbe essere un obiettivo chiave per semplificare la gestione delle crisi.

In merito all'art. 96 e all'obbligo di segnalazione di interferenze il numero di 30.000 clienti potenzialmente interessati proposti corrisponde a una città svizzera di medie dimensioni. Perciò, secondo il progetto presentato, una perturbazione che riguarda tutto il cantone di Appenzello Interno, che ha 16.300 abitanti, non sarebbe annunciata. È anche importante valutare la durata della perturbazione. Attualmente, le organizzazioni per le chiamate di emergenza considerano problematiche le interruzioni che possono interessare almeno 1.000 clienti per più di 15 minuti per cui riteniamo che questo valore sia più consono e cautelativo rispetto a quello proposto.

Si osserva inoltre che i compiti dell'Esercito svizzero in relazione alle minacce contro le infrastrutture critiche da parte di attacchi informatici di Stati terzi e alla difesa contro questi attacchi devono essere presentati e integrati nell'OST.
Già oggi, alcuni stati impiegano regolarmente i loro mezzi informatici nell'ottica di una "guerra fredda cibernetica". Nel caso di un conflitto armato in Europa (come peraltro dimostrato dal recente conflitto in Ucraina), occorre considerare che questi mezzi possono essere utilizzati su larga scala e che anche gli Stati non direttamente coinvolti nel conflitto possono potenzialmente esserne colpiti. Negli ultimi anni, l'esercito ha preso provvedimenti per prepararsi a un tale scenario. Per esempio, la Base d'aiuto alla condotta (BAC) nel settore della difesa è responsabile della pianificazione delle azioni, del monitoraggio della situazione, della gestione degli eventi così come della formazione del personale e dei militari in difesa da attacchi provenienti dal cyberspazio, dalla guerra elettronica e dalla crittologia. Con l'ulteriore sviluppo dell'Esercito (DEVA), è stata formata una compagnia informatica per sostenere l'organizzazione professionale della BAC. A partire dal 2022, tutta la formazione cyber dell'Esercito svizzero sarà integrata nel nuovo battaglione cyber 42. La revisione dell'OST deve dunque tenere conto del ruolo delle forze armate integrandone i compiti.

Le chiediamo, signora consigliera federale, di prendere in considerazione le nostre raccomandazioni.

Vogliate gradire, gentili signore ed egregi signori, i sensi della nostra massima stima.

PER IL CONSIGLIO DI STATO

Il Presidente	Il Cancelliere
Manuele Bertoli	Arnoldo Coduri

Copia a:
- Dipartimento delle istituzioni (di-dir@ti.ch)
- Dipartimento delle finanze e dell'economia (dfe-dir@ti.ch)
- Dipartimento del territorio (dt-dir@ti.ch)
- Divisione dell'ambiente (dt-da@ti.ch)
- Deputazione ticinese alle Camere federali (can-relazioniesterne@ti.ch)
- Pubblicazione in Internet