6 maggio 2024 | Ufficio federale della cibersicurezza UFCS

Rapporto semestrale 2023/II (luglio – dicembre)

Sicurezza delle informazioni

La situazione in Svizzera e a livello internazionale

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa,
della protezione della popolazione e dello sport DDPS
Ufficio federale della cibersicurezza UFCS

Panoramica / Contenuto

Management Summary

Il 1°gennaio 2024 il Centro nazionale per la cibersicurezza (NCSC) è stato trasferito all'Ufficio federale della cibersicurezza (UFCS). L'UFCS coglie l'opportunità di questa trasformazione per evidenziare, nel tema principale di questo rapporto, i diversi ambiti d'attività della Confederazione nel campo della cibersicurezza. I due contributi esterni mettono in luce le difficoltà che si incontrano nel perseguimento penale e le sfide legate alla certificazione della cibersicurezza nei Comuni.

Aumento delle segnalazioni nel secondo semestre 2023

Nel secondo semestre del 2023 l'allora NCSC ha ricevuto 30 331 segnalazioni di ciberincidenti, quasi il doppio rispetto allo stesso periodo del 2022 (16 951 segnalazioni). Questo aumento è dovuto principalmente a offerte di lavoro fraudolente e a chiamate fasulle a nome della polizia.

Anche nella seconda parte dell'anno le truffe si riconfermano al primo posto tra le segnalazioni ricevute dall'NCSC. I tentativi di truffa denunciati dalle imprese rientrano perlopiù nelle categorie «truffe del CEO», con 253 segnalazioni (stesso periodo dell'anno precedente: 190 segnalazioni), e «Business E-Mail Compromise (BEC)» (truffe con manipolazione delle fatture), con 63 segnalazioni (stesso periodo dell'anno precedente: 45 segnalazioni), e hanno registrato un lieve aumento. In calo, invece, gli attacchi ransomware segnalati ai danni delle imprese che, rispetto ai 54 del secondo semestre del 2022, nell'attuale periodo in rassegna sono scesi a quota 42.

Tentativi di truffa con l'intelligenza artificiale

Nel periodo in rassegna l'NCSC ha ricevuto un numero crescente di segnalazioni di tentate truffe in cui è stata utilizzata l'intelligenza artificiale (IA). Tra le casistiche denunciate, ad esempio, vi erano episodi di sextortion con immagini create con l'IA, telefonate e truffe sugli investimenti a nome di personaggi famosi. Visto il numero di segnalazioni relativamente ridotto in questo ambito, l'NCSC ritiene che si tratti ancora di primi tentativi da parte dei cibercriminali, attraverso cui sondare le possibilità future di utilizzare con profitto l'IA nei loro attacchi.

Il phishing si conferma il secondo fenomeno più segnalato

Rispetto allo stesso periodo dell'anno precedente le segnalazioni di phishing sono più che raddoppiate, passando da 2179 a ben 5536. Particolarmente degno di nota è il cosiddetto «chain phishing»: i phisher utilizzano account di posta elettronica hackerati per inviare e-mail a tutti gli indirizzi memorizzati in quella casella. Visto che il mittente dovrebbe essere noto ai destinatari, vi è una forte probabilità che questi ultimi cadano in trappola. A quel punto, dagli account violati viene nuovamente inviata un'e-mail a tutti i contatti della loro rubrica.

Editoriale

L'Ufficio federale della cibersicurezza: rafforzamento della cibersicurezza in Svizzera

Il 1° gennaio 2024 si è concluso il trasferimento del Centro nazionale per la cibersicurezza (NCSC) dal Dipartimento federale delle finanze (DFF) all'Ufficio federale della cibersicurezza (UFCS) presso il Dipartimento della difesa, della protezione della popolazione e dello sport (DDPS).

Il mandato principale rimane invariato anche nelle nuove vesti di ufficio federale: proteggere preventivamente la Svizzera dai ciber-rischi, fornire assistenza in caso di ciberincidenti e individuare le opportunità con cui garantire al Paese un buon posizionamento strategico nel ciberspazio. L'obiettivo primario è fare in modo che persone e organizzazioni siano consapevoli dei ciber-rischi e strutturino la cibersicurezza in funzione della propria propensione al rischio. A tal fine, insieme ai suoi partner l'UFCS ha il compito di mettere in atto meccanismi economici e sociali che, da un lato, riducano i rischi sistemici e, dall'altro, contengano il più possibile i costi associati alla lotta contro i ciber-rischi. In questo modo la Svizzera diventa una piazza interessante per le imprese che operano nel mondo digitale.

Alcune delle sfide attuali sul fronte della cibersicurezza nazionale riguardano l'elevata vulnerabilità dei sistemi informatici, una reattività ancora debole in caso di ciberincidenti e crisi di rilevanza sistemica, nonché una trasparenza spesso carente e l'assenza di dati per poter inquadrare e valutare criticamente le affermazioni di esperti e organizzazioni sul tema della cibersicurezza. Questi fattori di rischio fanno sì che i ciberattacchi vadano troppo spesso a buon fine, il che a sua volta si traduce in notevoli danni economici e in un alto rischio di interruzioni di servizio ai danni di infrastrutture critiche. Le segnalazioni di ciberattacchi con danni conseguenti aumentano in media di circa il 30 per cento all'anno. Sebbene questi numeri possano sembrare allarmanti, bisogna anche considerare che si tratta di una tendenza assolutamente comprensibile alla luce del crescente utilizzo dell'ambiente digitale. In un confronto internazionale, la Svizzera si colloca a metà classifica. La situazione va tuttavia presa sul serio e migliorata. A tal fine l'UFCS si concentra su quattro ambiti strategici: far comprendere le ciberminacce, mettere a disposizione strumenti per prevenire i ciberattacchi, ridurre i danni conseguenti e migliorare la sicurezza di prodotti e servizi digitali. Che cosa significhi in concreto tutto ciò può essere desunto dalla nuova strategia pubblicata dall'UFCS.

Un fattore di successo fondamentale per l'UFCS è il suo personale. L'UFCS vuole essere un datore di lavoro attraente per avere collaboratrici e collaboratori e attrarre nuovi talenti che sappiano orientare i prodotti e i servizi dell'UFCS alle esigenze della politica, dell'economia e della società civile con la massima efficienza e qualità possibile. Affinché ciò avvenga, l'UFCS dev'essere flessibile e in grado di adattare rapidamente la propria organizzazione a nuove esigenze e realtà economiche. Fondamentale in tal senso è consentire ai propri team di agire con la massima libertà possibile e far sì che le collaboratrici e i collaboratori in possesso delle competenze necessarie prendano le decisioni il più autonomamente possibile o possano quanto meno influenzarle in maniera significativa. Spesso si tratta di decisioni che devono essere prese in tempi rapidi, il che a sua volta implica una cultura dell'errore aperta e obiettiva. Personalmente preferisco commettere errori in maniera controllata e puntare sull'innovazione, piuttosto che non farne del tutto e rimanere in stallo. Altrettanto importante è tuttavia anche mantenere alta la «Operational Excellence», mettendo a segno risultati affidabili e coerenti. Il

fulcro di tutto ciò è un personale quanto più diversificato possibile, che continui a mettere in discussione sé stesso e la direzione dell'ufficio con uno spirito costruttivo. Non possiamo ancora dire di aver raggiunto questo traguardo ideale. Ma abbiamo compiuto passi importanti in questa direzione, il che si riflette anche nel proficuo lavoro che ritengo stiano facendo le nostre collaboratrici e i nostri collaboratori.

Per noi è importante che voi, care lettrici e cari lettori, ci diate un feedback e soprattutto che facciate anche della sana critica costruttiva se l'UFCS non soddisfa le vostre aspettative. In questa fase cruciale di sviluppo dell'Ufficio federale le vostre opinioni sono preziose come non mai. È insieme a voi, in fondo, che vogliamo creare un ciberspazio libero e sicuro a beneficio di tutti.

Florian Schütz, direttore dell'Ufficio federale della cibersicurezza

1 Tema principale: sfide nella cibersicurezza

La cibersicurezza, e quindi la protezione della Svizzera dai ciber-rischi, è un compito congiunto di società, economia e Stato. Tutte le parti coinvolte sono chiamate ad adottare misure adeguate in tal senso nella loro rispettiva sfera di competenza e influenza.

Come in molti settori, anche nel campo della cibersicurezza vale in primo luogo il principio della responsabilità personale. Esistono tuttavia sfide che vanno al di là delle capacità e delle possibilità della singola organizzazione o persona fisica, per cui spetta allo Stato intervenire fornendo assistenza o facendosi carico di determinate attività.

Con il Centro nazionale per la cibersicurezza (NCSC[1]) – l'odierno Ufficio federale della cibersicurezza (UFCS) che funge da centro di competenza della Confederazione per le ciberminacce – il Consiglio federale ha creato una struttura con cui poter affrontare a livello statale le varie sfide nel campo della cibersicurezza:

1.1 (Ri)conoscere le ciberminacce e informare in merito

Per sapere a cosa prestare attenzione e quali misure adottare, è importante conoscere i fenomeni del momento. Avere informazioni su ciò che sta accadendo e su quali siano gli sviluppi in corso aiuta a valutare i rischi e a prendere decisioni. Grazie alle segnalazioni ricevute dalla popolazione e dalle imprese (cfr. cap. 1.5 e cap. 2), ai contatti con i gestori di infrastrutture critiche (cfr. cap. 1.6) e a una rete nazionale e internazionale di organizzazioni partner, l'UFCS ha una buona visione d'insieme degli eventi e delle forme di minaccia attuali.

Queste informazioni sulla situazione, una volta filtrate per bacino d'utenza, vengono distribuite dall'UFCS alle diverse cerchie di destinatari con l'obiettivo di sensibilizzare (cfr. cap. 1.2) e consentire l'adozione di misure per la loro tutela (cfr. cap. 1.3 e 1.5).

Raccomandazioni:

Leggete i precedenti rapporti semestrali e visitate regolarmente il sito Internet dell'UFCS.

Anche su altri siti come cybercrimepolice.ch e «eBanking – ma sicuro!» (ebas.ch) è possibile trovare notizie di attualità su fenomeni, minacce e misure di protezione.

[1] National Cyber Security Centre, cfr. Finlandia: NCSC-FI (kyberturvallisuuskeskus.fi); Irlanda: National Cyber Security Centre (ncsc.gov.ie); Lettonia: National Cyber Security Centre (nksc.lt); Paesi Bassi: National Cyber Security Centre (ncsc.nl), Norvegia: Norwegian National Cyber Security Centre (nsm.no) e Regno Unito: National Cyber Security Centre (ncsc.gov.uk). In alcuni Paesi queste unità hanno denominazioni specifiche, come in Germania: BSI - Bundesamt für Sicherheit in der Informationstechnik (bsi.bund.de); in Francia: ANSSI - Agence nationale de la sécurité des systèmes d'information (cyber.gouv.fr) o negli USA: Cybersecurity & Infrastructure Security Agency – America's Cyber Defense Agency (cisa.gov). L'Australia e il Canada specificano invece il loro Paese nel nome: Australian Cyber Security Centre ACSC (cyber.gov.au) e Canadian Centre for Cyber Security CCCS (cyber.gc.ca). Si veda anche Centre for Cyber security Belgium (belgium.be) e Cyber Security Agency of Singapore (csa.gov.sg).

1.2 Sensibilizzazione

Le misure di sensibilizzazione e prevenzione sono basilari nella cibersicurezza, considerato il fatto che la gestione di un ciberincidente è notevolmente più complessa e dispendiosa rispetto, ad esempio, all'adozione di qualche misura di facile realizzazione con cui potersi muovere in sicurezza nello spazio digitale. Per tale motivo l'UFCS pubblica informazioni sulla cibersicurezza e fornisce raccomandazioni sulle misure preventive contro i ciberattacchi. Per la cyberstrategia nazionale (CSN), insieme a vari rappresentanti dell'economia, delle istituzioni, della popolazione e del mondo dell'istruzione sono stati definiti, da un lato, gli approcci con cui informare e sensibilizzare sulla tematica e, dall'altro, una serie di raccomandazioni operative specifiche per gruppo di destinatari circa le misure che le singole persone e organizzazioni possono adottare per proteggersi.

Per adempiere a questo compito in linea con le reali necessità, da un lato l'UFCS può sfruttare le conoscenze acquisite con le proprie attività operative. Dall'altro coordina a livello nazionale gli interventi mirati al miglioramento della ciberresilienza. Concepisce misure in stretta collaborazione con partner esterni quali la Prevenzione Svizzera della Criminalità, la piattaforma «e-banking – ma sicuro!» della Scuola universitaria professionale di Lucerna, la Swiss Internet Security Alliance e altre commissioni e organizzazioni esistenti. L'attuazione di queste misure e raccomandazioni può avvenire da parte dei singoli gruppi di destinatari individuati – che nel loro insieme rappresentano l'intera collettività – sotto la loro diretta responsabilità e in funzione del loro grado di coinvolgimento.

Per quanto riguarda l'economia, ad esempio, vengono realizzati singoli progetti pilota in settori quali la logistica, l'industria metalmeccanica o le imprese a conduzione familiare. In seguito, le informazioni e le conoscenze desunte da queste esperienze vengono idealmente discusse con le rispettive associazioni di categoria e quindi perfezionate e condivise con i relativi settori economici. Per quanto riguarda la popolazione, l'UFCS realizza insieme a partner esterni campagne nazionali con cui far conoscere meglio al grande pubblico contenuti rilevanti per la cibersicurezza e mettere a disposizione di ciascun utente di Internet e delle tecnologie digitali strumenti di facile applicazione con cui proteggersi dalla cibercriminalità durante la navigazione online. Tutte le iniziative vengono costantemente analizzate e verificate, in maniera tale da poterle ottimizzare dal punto di vista della loro realizzazione ed efficacia.

Raccomandazioni:

Informatevi regolarmente sugli eventi attuali che possono pregiudicare la vostra cibersicurezza o quella della vostra impresa. Sui siti dell'UFCS, della Prevenzione Svizzera della Criminalità PSC, «eBanking – ma sicuro!», della Piattaforma di sicurezza Internet iBarry o della campagna di prevenzione s-u-p-e-r.ch vi sono numerose informazioni per privati, imprese, autorità e specialisti IT.

Parlate con personale, parenti e conoscenti della cibersicurezza, della gestione dei dati e della cibercriminalità.

1.3 Fornire istruzioni su come proteggersi e incrementare la resilienza

In collaborazione con l'UFCS e l'economia, l'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) ha sviluppato lo standard minimo per le TIC, un compendio contenente istruzioni sistematiche per le imprese su come strutturare la propria cibersicurezza. Lo standard minimo per le TIC condensa vari standard riconosciuti a livello internazionale e, quale raccomandazione, vuole essere un contributo al miglioramento della resilienza TIC. Lo standard e il relativo tool di valutazione vengono regolarmente aggiornati.

Per vari settori critici, insieme ad associazioni e rappresentanti di categoria sono stati elaborati e pubblicati standard settoriali ai fini di un migliore allineamento con i requisiti specifici dei diversi settori. Anch'essi hanno, in linea di principio, carattere di raccomandazione.

In certi settori, alcuni aspetti dello standard minimo per le TIC sono anche stati prescritti come vincolanti. È il caso, ad esempio, degli standard minimi TIC per le forniture di elettricità e gas, dichiarati obbligatori dall'Ufficio federale dell'energia (UFE). L'obbligo è in vigore dal 2024 per l'elettricità, mentre per il gas scatterà dal 2025. L'Ufficio federale dei trasporti (UFT) ha pubblicato la direttiva sulla cibersicurezza in ambito ferroviario (D CySec-Rail) nell'autunno del 2023. La nuova direttiva descrive i requisiti minimi per un sistema di gestione della sicurezza delle informazioni (ISMS) che le imprese ferroviarie devono istituire e mantenere. La direttiva CySec-Rail, che entrerà in vigore il 1° luglio 2024, fa riferimento allo "standard minimo TIC per i trasporti pubblici", pubblicato dal 2020.[2]

Da parte sua, l'UFCS contribuisce con istruzioni e raccomandazioni inerenti a vari temi, quali ad esempio la sicurezza dei siti web[3], la protezione dei sistemi di controllo industriali[4] e dei dispositivi dell'«Internet delle cose»[5], o alla collaborazione con i fornitori di servizi informatici[6].

Conclusione / raccomandazione:

Sul sito Internet dell'UFCS sono disponibili numerose informazioni sulla cibersicurezza.

Gli standard minimi per le TIC e gli standard minimi per diversi settori fungono da raccomandazione e orientamento per proteggersi dalle minacce dei ciber-rischi.

1.4 Marchio cyber-safe.ch – esperienze di un Comune vodese

Contributo ospite di Kilian Cuche, consigliere comunale di Pomy/VD

Dopo circa due anni e mezzo di lavoro, a fine 2023 il Comune di Pomy nel distretto del Giura Nord vodese, che conta in tutto 900 abitanti, ha ottenuto il marchio di cibersicurezza svizzero cyber-safe.ch. Questo articolo spiega le varie fasi del processo, dal rilevamento dello stato di

---

2 Direttiva sulla cibersicurezza (bav.admin.ch)

3 Misure a protezione dei sistemi di gestione dei contenuti (CMS) (ncsc.admin.ch); Misure contro gli attacchi DDoS (ncsc.admin.ch)

4 Misure di protezione dei sistemi di controllo industriali (ICS) (ncsc.admin.ch)

5 Sicurezza nell'Internet delle cose (IoT) (ncsc.admin.ch)

6 Collaborazione con i fornitori di servizi informatici (ncsc.admin.ch)

fatto ai vantaggi dell'applicazione del marchio, mettendo in luce le sfide e le opportunità per i Comuni.

1.4.1 La fase di maturazione della consapevolezza nei confronti della cibersicurezza

Nel 2021, dopo un evento organizzato dall'Unione dei Comuni Vodesi (UCV) sul tema della cibersicurezza, è nata l'idea di fare il punto della situazione nel Comune di Pomy e introdurre eventuali miglioramenti. Alla conferenza era stato presentato il marchio cyber-safe.ch, che ci ha dato lo spunto per lanciare l'iniziativa. Naturalmente bisognava innanzitutto convincere l'intero consiglio comunale a investire nella cibersicurezza. A tale proposito, sulla base di un primo questionario l'associazione cyber-safe.ch ci ha quantificato i costi che potrebbero insorgere in caso di ciberattacco, considerata l'entità della nostra infrastruttura e la mole dei nostri dati. Questo resoconto è stato estremamente utile nell'evidenziare il rapporto costi-benefici di un investimento nella cibersicurezza. Ben presto il Comune di Pomy si è convinto della necessità dell'investimento e, nella primavera del 2021, ha avviato le pratiche per l'ottenimento del marchio. Il ciberattacco subito qualche mese dopo dal Comune di Rolle non ha fatto altro che accrescere ulteriormente la nostra volontà di migliorare il livello di cibersicurezza comunale.

1.4.2 Il processo di ottenimento del marchio cyber-safe.ch

Il primo passo verso l'ottenimento del marchio cyber-safe.ch è stata la redazione di un rapporto sulla base di questionari, test di phishing e di un'analisi della nostra infrastruttura informatica (scansione per individuare eventuali falle di sicurezza). Con quel documento è stato rilevato lo stato di fatto della cibersicurezza all'interno del Comune e sono state definite le misure prioritarie da adottare quali presupposti per l'ottenimento del marchio. In altre parole abbiamo ricevuto un elenco di punti soddisfatti e non soddisfatti, sulla base del quale potevano redigere un piano d'azione per prepararci alla certificazione. A quel punto siamo giunti alla parte più importante del lavoro: l'attuazione delle misure correttive. Dalla gestione degli aggiornamenti al controllo dei backup, alla formazione degli utenti, fino alla protezione fisica della nostra infrastruttura – tutti gli elementi essenziali della cibersicurezza sono stati esaminati, controllati, adeguati e corretti. Due anni dopo ci siamo sottoposti a un primo audit, in cui sono state riscontrate ancora alcune non conformità. Una volta eliminate, siamo riusciti, dopo un secondo audit, a ottenere la certificazione cyber-safe.ch.

1.4.3 Vantaggi, sfide e opportunità per i Comuni

Il marchio cyber-safe.ch è stato per noi un ottimo strumento con cui migliorare la cibersicurezza. Grazie a un punto di vista sull'infrastruttura comunale indipendente dalla nostra amministrazione e dal nostro fornitore di servizi informatici, siamo riusciti a cogliere pienamente e in tutte le sue sfaccettature il potenziale miglioramento. Siamo stati assistiti con professionalità, ma anche con un atteggiamento di comprensione per le sfide tipiche dei piccoli Comuni. Una di esse, in particolare, è il fatto che il nostro consiglio comunale è costituito esclusivamente da politici di milizia, che hanno risorse limitate in termini di tempo, di competenze ma anche di conoscenze in materia di cibersicurezza. Tutti queste specificità sono state prese in considerazione, trovando una soluzione su misura per il nostro contesto particolare. Fa anche piacere vedere come molti Cantoni stiano mettendo a disposizione dei Comuni sempre più risorse per aiutarli a migliorare la cibersicurezza. Questi sforzi dovrebbero essere estesi e coordinati a livello nazionale.

1.4.4 Conclusione

Nonostante la nostra infrastruttura – con due postazioni di lavoro, un server e alcuni dispositivi BYOD[7] – sia molto piccola, la mole di lavoro necessaria per l'ottenimento di un marchio di cibersicurezza come cyber-safe.ch non è da sottovalutare. La maggior parte delle misure dipende in realtà dalle dimensioni dell'infrastruttura. I responsabili del marchio ci hanno tuttavia assistito in maniera pragmatica, adeguandosi alle nostre necessità e alle diverse realtà locali. Ottenere il marchio non è dunque una «mission impossible». Con un buon accompagnamento, un change management nei confronti del personale e il supporto dei fornitori di servizi informatici, il miglioramento della cibersicurezza è un traguardo raggiungibile da tutti i Comuni svizzeri e un punto che dovrebbe far parte di ogni pianificazione informatica comunale. In fondo si tratta della sicurezza dei dati dei nostri cittadini e della protezione delle infrastrutture critiche di responsabilità dei Comuni.

1.5 Registrare gli incidenti e dare consigli a chi è coinvolto

L'UFCS riceve segnalazioni riguardanti ciberincidenti e ciberminacce. A tale scopo gestisce il Servizio nazionale di contatto per le ciberminacce, classificando le segnalazioni ricevute ed effettuando una prima analisi in base alla quale adottare misure e svolgere eventuali ulteriori indagini di approfondimento. Gli autori delle segnalazioni vengono assistiti nella maniera più rapida, semplice e competente possibile: oltre a rispondere direttamente alle loro domande, si danno loro consigli su come procedere e/o li si indirizza ai servizi competenti. In veste di referente nazionale e centrale per le segnalazioni e le domande legate al mondo ciber, l'UFCS collabora a stretto contatto con vari attori di Confederazione, Cantoni, autorità di perseguimento penale, ma anche con soggetti privati – tra cui ad esempio i fornitori di servizi – partner e organizzazioni internazionali. L'UFCS assicura inoltre che siti web, indirizzi e-mail, numeri di telefono ecc. fraudolenti vengano comunicati ai servizi competenti, affinché questi ultimi possano adottare i provvedimenti del caso.

In base alle segnalazioni ricevute, l'UFCS individua nuove tendenze e strategie in ambito ciber e ricava una panoramica generale dei casi che completa il quadro complessivo della situazione attuale nel ciberspazio (cfr. cap. 1.1). L'evoluzione di questi fenomeni viene costantemente analizzata, in maniera tale da poter avvisare la popolazione e le imprese in caso di un'escalation della minaccia. I numeri raccolti costituiscono una base di riferimento importante per la prevenzione e la sensibilizzazione dell'opinione pubblica nei confronti dei ciber-rischi (cfr. cap. 1.2), da cui trarre informazioni con cui prevenire futuri reati ed evitare ulteriori vittime.

Raccomandazioni:

Contribuite a riconoscere i rischi su Internet, comunicando incidenti e ciberminacce all'UFCS mediante il modulo di segnalazione: NCSC Report (ncsc.admin.ch)

[7] BYOD significa «bring your own device», cfr. Bring your own device (wikipedia.org)

1.6 Proteggere e sostenere le infrastrutture critiche

Le infrastrutture critiche sono processi, sistemi e installazioni essenziali per il funzionamento dell'economia e il benessere della popolazione. L'UFCS sostiene i gestori di infrastrutture critiche in Svizzera nella protezione contro le ciberminacce e quindi nella minimizzazione dei rischi informatici; gestisce a tale scopo il team nazionale di risposta alle emergenze informatiche (Computer Emergency Response Team [CERT]), che funge da servizio specialistico incaricato della gestione tecnica dei ciberincidenti e dell'analisi tecnica delle ciberminacce.

Ai gestori di infrastrutture critiche l'UFCS mette a disposizione strumenti e dati con cui incrementare la cibersicurezza dei loro servizi e dei rispettivi utenti, ad esempio informazioni tecniche sulle infrastrutture informatiche utilizzate abusivamente per diffondere software dannosi (i cosiddetti «malware») o gestire siti web di phishing.

1.7 Ridurre le vulnerabilità

Software e/o configurazioni di sistema possono presentare dei punti deboli che gli aggressori sfruttano per procurarsi un accesso non autorizzato. Per ridurre la superficie d'attacco e prevenire gli incidenti, occorre individuare ed eliminare rapidamente tali vulnerabilità.

Dai propri partner e tramite diverse fonti interne ed esterne, l'UFCS riceve quotidianamente indicazioni sui possibili punti deboli presenti all'interno dei sistemi informatici. Tali informazioni vengono esaminate attentamente, dopodiché dalle singole segnalazioni – una volta completata l'analisi – vengono ricavate le misure necessarie per i sistemi della Confederazione e per eventuali servizi esterni. Dalla propria piattaforma informativa, ad esempio, l'UFCS ha la possibilità di avvisare i gestori di infrastrutture critiche dell'esistenza di determinate falle di sicurezza e pubblicare avvisi di sicurezza rilevanti.

Spesso, inoltre, l'UFCS informa le imprese interessate anche direttamente via e-mail, per telefono o lettera raccomandata. Così facendo, insieme a loro si riesce in molti casi a rimediare per tempo alle criticità e a colmare le lacune.

L'UFCS è inoltre il servizio ufficiale di contatto per segnalare le falle di sicurezza in Svizzera ed è riconosciuto dal MITRE[8] come servizio autorizzato ad assegnare numeri CVE. In questa funzione l'UFCS, assicurando la pubblicazione coordinata delle criticità che gli sono state segnalate, contribuisce in maniera determinante a prevenire per quanto possibile lo sfruttamento di queste vulnerabilità.[9]

Anche le misure di sensibilizzazione sono utili a ridurre la superficie d'attacco. L'UFCS incoraggia ad esempio le imprese, organizzazioni e amministrazioni svizzere a implementare lo standard di sicurezza security.txt[10], fornendo così un contributo fondamentale alla cibersicurezza.

Per migliorare la cibersicurezza dell'infrastruttura informatica della Confederazione e ridurre i ciber-rischi, l'UFCS è anche responsabile della gestione del proprio programma «bug bounty».

---

8 Solving Problems for a Safer World (mitre.org)

9 L'NCSC fa ora parte della rete mondiale per la gestione delle vulnerabilità nei sistemi informatici (ncsc.admin.ch)

10 Security.txt - Pubblicare sul sito web il contatto della persona responsabile della sicurezza (ncsc.admin.ch)

A complemento di altre misure volte a garantire la sicurezza, i programmi «bug bounty» servono a identificare, documentare ed eliminare eventuali vulnerabilità nei sistemi informatici grazie alla collaborazione con hacker etici.

Raccomandazioni:

Effettuate gli aggiornamenti delle app e dei programmi installati non appena disponibili. Attivate possibilmente la funzione di aggiornamento automatica.

Considerate il ciclo di vita di dispositivi e software, sostituendoli nel momento in cui il produttore non fornisce più aggiornamenti sulla sicurezza.

Per le imprese: tenete un inventario aggiornato dell'hardware e del software installato e assicuratevi di ricevere le informazioni su falle di sicurezza e relativi aggiornamenti.

1.8 Il perseguimento penale della cibercriminalità

Contributo ospite di Serdar Günal Rütsche, responsabile della Rete nazionale di sostegno alle indagini nella lotta contro la criminalità digitale (NEDIK)

Attualmente il ransomware rappresenta la minaccia di gran lunga più preoccupante nel campo della cibercriminalità in Svizzera. Nonostante il livello di protezione del nostro Paese sia già in realtà molto buono, chi utilizza i servizi Internet – siano essi imprese o soggetti privati – si espone a questa tipologia di attacchi. La digitalizzazione offre all'economia nuove opportunità di crescita e possibilità di occupazione. Al contempo, richiede nuovi processi che comportano necessariamente una maggiore dipendenza da una tecnologia dell'informazione e della comunicazione ben funzionante. Queste interdipendenze vengono sfruttate anche dai criminali. Sono sempre più sofisticati i metodi che questi ultimi utilizzano per insinuarsi nelle reti, sottrarre i dati o paralizzare interi sistemi. Che si tratti di piccole ditte artigianali o di grandi aziende, un ciberattacco può rivelarsi letale per chiunque.

Il numero di reati denunciati nell'ambito della cibercriminalità e della criminalità digitale ha subìto un'impennata nel 2023, soprattutto nel campo della cibercriminalità economica. Le minacce nel ciberspazio rappresentano uno dei pericoli più significativi per imprese, autorità, persone fisiche e infrastrutture critiche. Il progresso tecnologico nel campo dell'IA offre ai criminali nuovi vettori d'attacco che, potendo essere utilizzati per una molteplicità di applicazioni, li facilitano nel loro intento. La Rete nazionale di sostegno alle indagini nella lotta contro la criminalità digitale (NEDIK), frutto della collaborazione tra i corpi di polizia svizzeri, è nata per combattere insieme la criminalità digitale e la cibercriminalità. A tal fine si occupa di coordinare la gestione dei casi, scambiare le informazioni in tempi rapidi, redigere prospetti aggiornati e nazionali dei ciberincidenti, condividere le conoscenze di base e sviluppare progetti intercantonali in cooperazione con i partner nazionali e internazionali rilevanti. Tutti i corpi di polizia forniscono il loro contributo. Grazie alla creazione di una piattaforma interdisciplinare di questo tipo è possibile individuare sul nascere, e contrastare, fenomeni e minacce. Attraverso la collaborazione attiva, la costituzione di nuove partnership e un'attività di prevenzione sul campo si mira a contenere la criminalità nello spazio digitale e a proteggere la popolazione svizzera. Nel 2023 la NEDIK ha sostenuto vari progetti sul tema, ad esempio nel campo delle truffe sugli investimenti online e della pedocriminalità, puntando a rafforzare la collaborazione con leader del mercato appartenenti al mondo civile.

Negli anni a venire assisteremo a cambiamenti radicali nell'ambito della cibercriminalità. Il ransomware rimarrà una minaccia cruciale per la Svizzera, per cui dovremo continuare a lavorare sulla sensibilizzazione della popolazione. L'IA cambierà radicalmente la situazione sul fronte delle minacce: con nuove possibilità d'attacco come il voice cloning o i deepfake, il ventaglio di opzioni a disposizione dei criminali si sta ampliando massicciamente. L'IA, da sola, non riesce a creare da un malware esistente una ciberminaccia completamente nuova, ma con la collaborazione dell'essere umano è possibile. Grazie all'IA, inoltre, i reati di truffa stanno diventando sempre più sofisticati e personalizzati. Per proteggerci da queste minacce, dobbiamo continuare a puntare su team di sicurezza altamente specializzati e su una gestione consapevole dei dati, stanziando budget adeguati, creando posti di formazione sul territorio nazionale e perfezionando il quadro normativo. La sicurezza informatica non è solo una questione di tecnologia, ma un compito collettivo che presuppone cooperazioni vincolanti.

2 Segnalazioni provenienti da imprese e privati

2.1 Segnalazioni di ciberincidenti ricevute

Nel 2023 il numero complessivo di segnalazioni ricevute dall'NCSC e dall'odierno UFCS è nuovamente cresciuto. Con 49 380 segnalazioni, l'aumento rispetto all'anno scorso (34 527 segnalazioni) è stato significativo. Nel secondo semestre del 2023 l'impennata rispetto all'anno precedente è ancora più marcata: mentre negli ultimi sei mesi del 2022 le segnalazioni pervenute erano state 16 951, nel periodo in esame se ne sono registrate ben 30 331. Questa crescita pari quasi al doppio è dovuta principalmente all'aumento di due fenomeni: le «offerte di lavoro fraudolente»[11] e le «chiamate fasulle a nome della polizia»[12].

Il rapporto tra le segnalazioni provenienti da privati (88%) e quelle da parte di imprese, associazioni e autorità (12%) continua invece a mantenersi stabile. Tra i reati di frode tipicamente segnalati dalle imprese – le truffe dei CEO[13] e le frodi con manipolazione delle fatture[14] – si registra un lieve aumento nella seconda metà dell'anno. Nel caso della truffa del CEO il numero di segnalazioni pervenute nel secondo semestre del 2023 è cresciuto da 190 a 253 rispetto allo stesso periodo del 2022, mentre per quanto riguarda il secondo caso – il cosiddetto «Business E-Mail Compromise (BEC)» – le segnalazioni sono passate da 45 a 63. Per quanto riguarda gli attacchi ransomware[15] ai danni delle imprese, nel secondo semestre le segnalazioni hanno segnato un lieve calo: mentre negli ultimi sei mesi del 2022 l'NCSC ne aveva ricevute 54, nel periodo in esame sono state soltanto 42. In forte calo, invece, gli attacchi ransomware a privati – soltanto 3 nel secondo semestre del 2023 rispetto ai 22 segnalati nello stesso periodo dell'anno scorso.

11 Offerte di lavoro fraudolente (ncsc.admin.ch)
12 Chiamate a nome di false autorità (polizia, dogana) (ncsc.admin.ch)
13 Truffa del CEO (ncsc.admin.ch)
14 Business E-Mail Compromise (BEC) (ncsc.admin.ch)
15 Ransomware (ncsc.admin.ch)

Segnalazioni settimanali pervenute all'NCSC nel secondo semestre del 2023

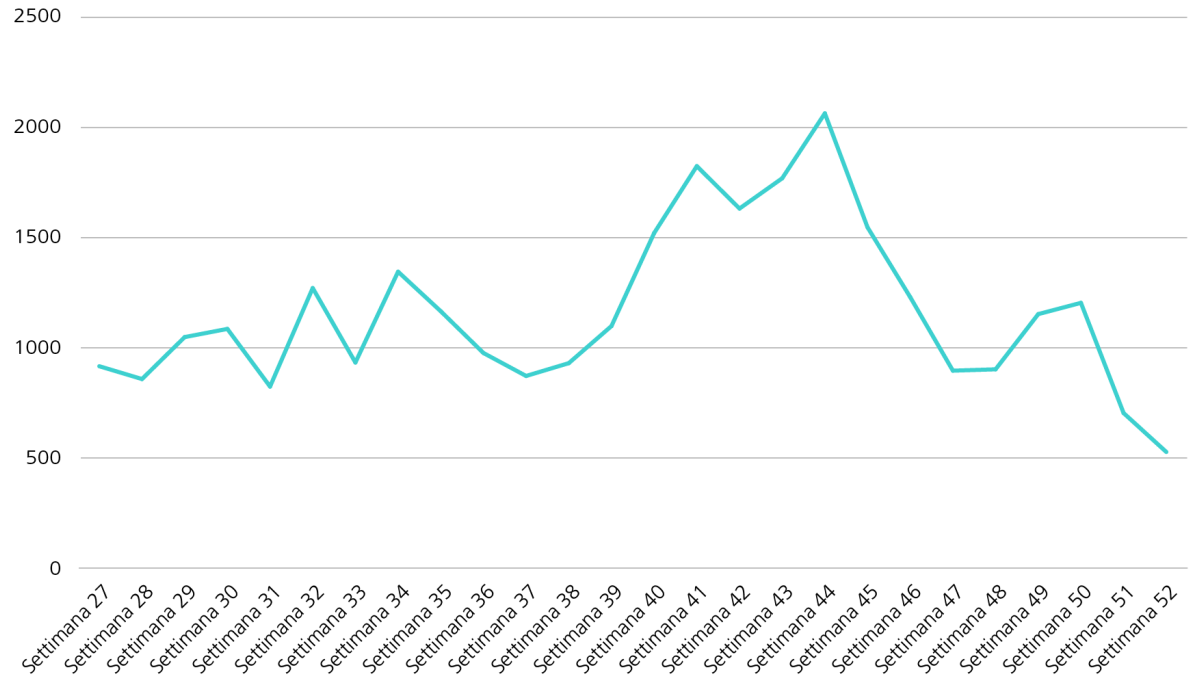

Fig. 1: Segnalazioni settimanali all'NCSC tra luglio e dicembre 2023, vedi anche Numeri attuali (ncsc.admin.ch).

Segnalazioni pervenute all'NCSC nel secondo semestre del 2023 per categoria

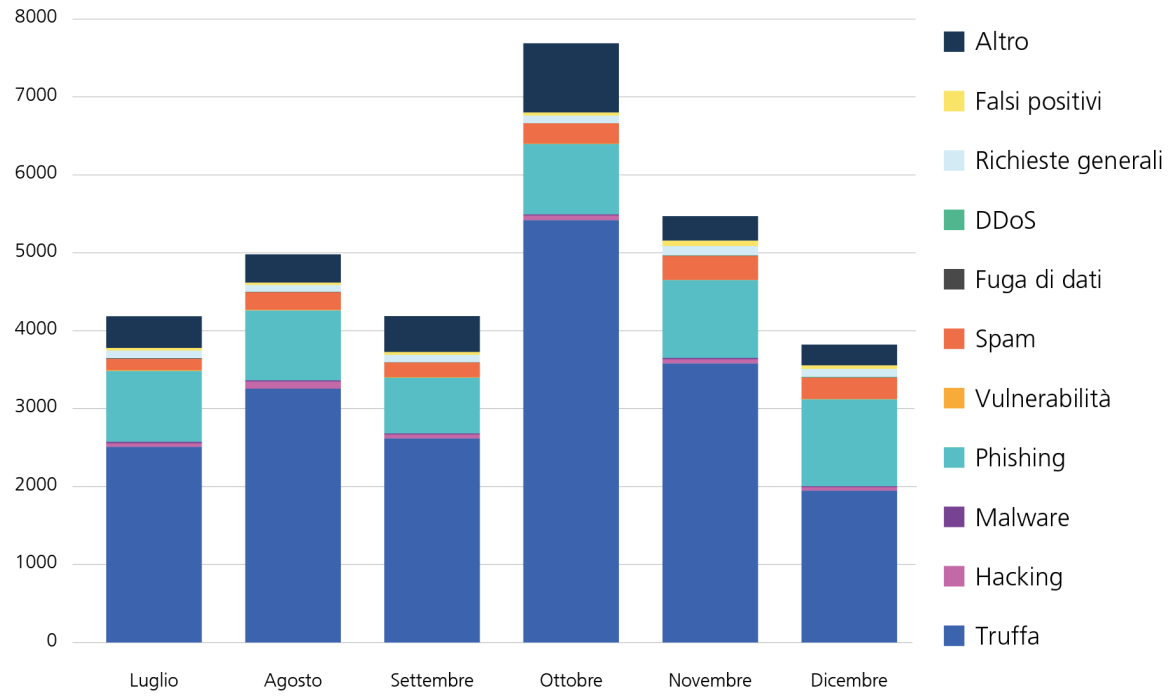

Fig. 2: Segnalazioni all'NCSC nel primo semestre del 2023 per categoria, vedi anche Numeri attuali (ncsc.admin.ch).

2.2 Truffa

2.2.1 La truffa si riconferma al primo posto per numero di segnalazioni

Anche nel 2023 le truffe si riconfermano, con oltre 30 000 segnalazioni, il fenomeno di gran lunga più frequente. Colpisce in particolare l'aumento registrato nel secondo semestre dell'anno. Rispetto agli ultimi sei mesi del 2022 il numero di segnalazioni è praticamente raddoppiato, salendo da 10 503 a ben 19 323. Come già registrato in passato, buona parte di esse ha riguardato e-mail minatorie inviate da presunte autorità di perseguimento penale. Nel secondo semestre del 2023 sono state 4461 le segnalazioni ricevute in tale ambito. Si tratta di e-mail minatorie in cui si comunica alla vittima che è ritenuta colpevole di un grave reato (in genere legato alla pornografia minorile) e che l'unico modo per evitare un'azione penale è versare una somma di denaro.[16]

Nella seconda metà dell'anno ha preso piede un diverso modus operandi che ha fatto lievitare il numero di segnalazioni. La variante inizia con una telefonata da parte di una presunta autorità di polizia. Una voce sintetica informa il malcapitato del fatto che, ad esempio, i dati del suo conto corrente privato sono emersi in relazione a un dato reato. Per avere ulteriori informazioni, deve premere il tasto 1. Se la vittima preme 1, la chiamata viene inoltrata a un «operatore» che gli chiede di scaricare uno strumento di accesso remoto, il che consente al criminale di insinuarsi nel computer o nel telefono cellulare. Una volta entrati, gli aggressori cercano di accedere alle credenziali di e-banking della vittima, così da prelevare in background denaro dal conto tramite lo strumento di accesso remoto. Nel secondo semestre del 2023 le segnalazioni relative a questo fenomeno sono aumentate in maniera esponenziale. Il picco è stato raggiunto nella settimana 44, quando l'NCSC ha registrato la cifra record di 2059 segnalazioni, di cui circa la metà – 914 – riguardavano telefonate minatorie.[17]

Nel secondo semestre dell'anno sono cresciute anche le segnalazioni relative a offerte di lavoro fasulle. Le offerte, provenienti da presunte agenzie di collocamento, sono state inviate principalmente via WhatsApp, attirando le candidate e i candidati con promesse di guadagni straordinari. Tramite una piattaforma online, le «collaboratrici» e i «collaboratori» ricevevano un elenco di mandati, ad es. redigere recensioni di prodotti. Per ogni recensione si riceveva un determinato compenso, che veniva accreditato tramite la piattaforma sull'account del collaboratore. Tuttavia il numero di mandati disponibili si azzerava rapidamente. Per accelerare l'attività e non dover aspettare, la piattaforma dava la possibilità di generare a pagamento nuovi mandati. Per pochi dollari si potevano così acquistare 50 nuovi mandati di recensione. Il guadagno promesso, che a sua volta avrebbe dovuto essere accreditato sulla piattaforma, superava di molto i costi, per cui la vittima pensava che valesse la pena utilizzare quel modello. La brutta sorpresa arrivava quando si voleva incassare il guadagno accumulato. Il gestore della piattaforma richiedeva delle tasse per il versamento del guadagno finché la vittima si accorgeva che si trattava di una truffa.[18]

---

16 Finte e-mail minatorie a nome delle autorità (ncsc.admin.ch)

17 Settimana 43: «strutture organizzative» della falsa assistenza (ncsc.admin.ch)

18 Settimana 35: finte offerte di lavoro 2.0 (ncsc.admin.ch)

2.2.2 Primi tentativi di truffa con l'IA

Nell'ultimo anno l'IA è diventato un argomento di tendenza e con ChatGTP ha definitivamente conquistato anche il pubblico più ampio. Come ogni tecnologia, se da un lato può essere sfruttata con profitto, dall'altro può anche arrecare danni. Non c'è dunque da sorprendersi se anche i cibercriminali cerchino di approfittare dell'IA per i loro scopi. In base ai casi segnalati, l'UFCS ritiene tuttavia che non se ne stia ancora facendo un uso sistematico. Si tratta piuttosto di tentativi con cui i truffatori cercano di sondare cosa sia possibile o redditizio.[19]

2.2.2.1 Sextortion con immagini create con l'IA

Il termine sextortion designa un metodo di estorsione per mezzo di immagini o filmati che mostrano la vittima mentre compie atti di natura sessuale e/o nuda. Le vittime vengono contattate tramite le reti sociali da parte di una donna o un uomo attraente e quindi indotte a spogliarsi davanti alla telecamera. Tutte queste azioni vengono riprese di nascosto. In seguito la vittima viene ricattata con la minaccia di pubblicare i filmati su YouTube indicando il suo nome o di inviare le registrazioni via e-mail a familiari, amici o al datore di lavoro.[20]

All'UFCS sono noti anche casi in cui l'IA viene utilizzata per creare foto o video compromettenti allo scopo di ricattare la vittima. Basta che i criminali siano in possesso di filmati o fotografie del tutto innocenti registrate o scattate personalmente dalla vittima in precedenza o magari accessibili a tutti su Internet. Da questi video innocui l'IA crea filmati pornografici o immagini di nudo. Le possibilità che offre questa tecnologia sono diventate definitivamente note a tutti con i deepfake porno di Taylor Swift[21]. L'UFCS ritiene che questa forma di estorsione crescerà vertiginosamente negli anni a venire. Accanto a questo scenario cupo, c'è però anche un aspetto positivo. Dato che questi falsi video possono essere creati ai danni praticamente di chiunque sia presente su Internet con foto e video, il fenomeno potrebbe ridimensionarsi, il che significa che l'ipotesi di minaccia potrebbe affievolirsi anche per coloro di cui esistono effettivamente video compromettenti.

2.2.2.2 Telefonate

La maggior parte dei tentativi di frode continua a essere perpetrata per iscritto, tramite e-mail o servizi di messaggistica; solo una minoranza avviene per telefono. Il motivo è ovvio: mentre nella comunicazione scritta gli aggressori hanno tempo a sufficienza per tradurre i loro messaggi nella lingua in questione tramite Deepl o altro, in caso di telefonata bisogna conoscere la lingua ed essere in grado di interloquire direttamente con la vittima. In futuro l'IA potrebbe prendere piede anche in questo ambito, traducendo simultaneamente le telefonate con una voce e una lingua predefinite. I primi segnali in tal senso esistono già: varie imprese, infatti, hanno segnalato all'UFCS di aver ricevuto telefonate da loro presunti dipendenti che, con voce perfettamente simulata, si sarebbero informati su questioni aziendali interne o avrebbero disposto l'esecuzione di pagamenti. I dipendenti in questione, tuttavia, erano completamente ignari di queste telefonate, che con tutta probabilità vengono generate tramite deepfake. Anche nelle telefonate shock ai genitori su presunti incidenti ai loro figli si utilizzano voci molto

---

19 Settimana 49: impiego dell'IA a scopo di truffa (ncsc.admin.ch)

20 Sextortion (ncsc.admin.ch); Prevenzione Svizzera della Criminalità | Sextortion (skppsc.ch)

21 Deepfake-Pornos: Ein manipuliertes Video kann ein Leben ruinieren (srf.ch)

simili a quelle dei ragazzi. In questo caso, tuttavia, non si sa esattamente quanto peso abbia già l'IA.

2.2.2.3 Comunicazione in svizzero tedesco

In alcuni casi sporadici compaiono anche e-mail di phishing in svizzero tedesco, come peraltro già riferito dall'NCSC nell'ultimo semestre.[22] Anche dietro queste e-mail potrebbe celarsi l'IA. È una scelta, tuttavia, alquanto sorprendente. Nel mondo degli affari, infatti, si utilizza di prassi il tedesco standard. Una presunta e-mail ufficiale proveniente da una banca e scritta in dialetto tenderebbe a insospettire la vittima piuttosto che convincerla a cliccare sul relativo link. Dovrebbe dunque essersi trattato di semplici tentativi da parte dei truffatori. C'è però un altro settore in cui il dialetto è comunemente utilizzato nella comunicazione: sono le truffe legate ai piccoli annunci, nell'ambito delle quali lo scorso semestre l'NCSC aveva osservato alcuni casi di utilizzo del dialetto. Questo stratagemma infonde fiducia nella vittima, dando l'impressione che acquirente e venditore provengano dalla medesima regione (linguistica). Si presume che in questi casi si utilizzi anche l'IA.

2.2.2.4 Truffa degli investimenti con personaggi famosi

Nel caso delle truffe sugli investimenti online si utilizzano spesso foto di personaggi famosi per dare una parvenza di serietà a offerte poco convincenti. Le foto o i video impiegati non sono necessariamente solo quelli pubblici; vengono anche generati filmati deepfake. Un esempio è stato il video promozionale falso di Elon Musk in occasione del lancio del razzo Starship. Gli aggressori hanno approfittato del lancio di Starship da parte di SpaceX, azienda di Elon Musk, come occasione per pubblicizzare una truffa «give away». Su un sito Internet, Elon Musk promette di rimborsare il doppio dell'importo corrispondente in criptovalute versatogli in occasione del lancio.[23]

Conclusioni / raccomandazioni:

Con l'ausilio di applicazioni IA si possono creare contenuti per e-mail e messaggi di testo apparentemente credibili che, a livello di lingua e di forma, assomigliano in tutto e per tutto a una comunicazione legittima e sono praticamente impossibili da distinguere dall'opera di una persona con padronanza linguistica. Per i destinatari di questi contenuti è quindi difficile capire che si tratta di tentativi di truffa.

L'impiego dell'IA, inoltre, consente di generare foto e video apparentemente autentici e voci che sembrano reali (i cosiddetti «deepfake»). Questi strumenti possono essere utilizzati per attacchi di social engineering. Le imitazioni delle voci possono convincere i malcapitati di parlare con un conoscente che ha bisogno di denaro o di un altro tipo di aiuto.

I truffatori pensano a sempre nuovi scenari per indurre le vittime ad agire in maniera avventata. Attraverso il social engineering e i contenuti generati con l'IA si vuole fare in modo che le vittime compiano atti pilotati dai criminali senza nutrire alcun sospetto. Non fatevi cogliere di

[22] Settimana 14: E-mail di phishing redatte in svizzero tedesco e una fattura a nome della Guardia terrestre svizzera di soccorso (ncsc.admin.ch)

[23] Settimana 17: video promozionale falso per una truffa «give away» (ncsc.admin.ch)

sorpresa, dunque, ma riflettete con calma e, in caso di dubbio, chiedete un parere ad altre persone o all'UFCS.

2.3 Segnalazioni di phishing

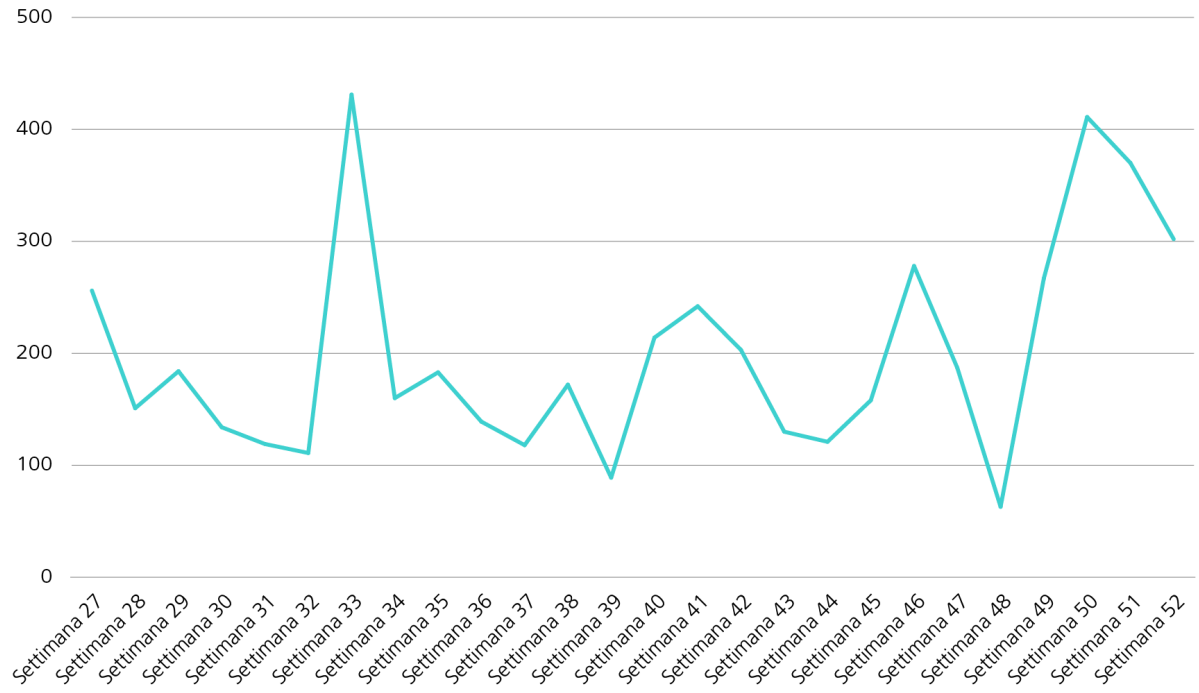

Fig. 3: Numero di URL di phishing verificati e confermati settimanalmente dall'NCSC nel secondo semestre 2023.

2.3.1 Chain-phishing, phishing effettuato tramite pacchi e pagamenti doppi delle fatture

Dopo la truffa, il phishing si conferma al secondo posto tra i fenomeni più segnalati mediante l'apposito modulo. Rispetto allo stesso periodo dell'anno scorso, il numero di segnalazioni in merito è più che raddoppiato, passando nel secondo semestre del 2023 da 2179 a 5536. Nell'arco dei 12 mesi l'NCSC ha ricevuto con questa modalità ben 9415 segnalazioni di phishing. Un altro canale di trasmissione messo a disposizione dall'NCSC (oggi UFCS) è la piattaforma antiphishing.ch, dove le segnalazioni di phishing vengono elaborate in maniera parzialmente automatizzata.[24]

Nella maggior parte dei casi si tratta di invii di massa, contenenti errori e diffusi senza particolari sforzi. Un tipico segnale, ad esempio, è ancora oggi l'uso di un appellativo impersonale come «Caro cliente» o addirittura l'assenza di un appellativo e il semplice «indirizzo e-mail».

I tentativi di phishing più segnalati sono gli stessi dell'anno scorso. Continuano a essere inviati migliaia di messaggi fraudolenti concernenti la consegna di un pacco[25]. Anche le e-mail che

[24] Si veda in merito anche il Rapporto anti-phishing 2023 (ncsc.admin.ch).

[25] Abbonamento trappola pacchetto (ncsc.admin.ch); Settimana 23: dal tentativo di phishing all'abbonamento trappola (ncsc.admin.ch); si veda anche Rapporto anti-phishing 2023 (ncsc.admin.ch)

annunciano un presunto rimborso a nome di provider, da parte delle FFS o dell'Amministrazione delle contribuzioni rientrano nel repertorio standard dei phisher.[26] In questo caso gli aggressori contano soprattutto sull'elevata probabilità che qualcuno stia effettivamente aspettando la consegna di un pacco o che abbia pagato la fattura emessa da un provider o da qualcun altro. Ciò conferisce una maggiore credibilità all'e-mail.

D'altro lato l'UFCS rileva un aumento degli attacchi di phishing rivolti alle imprese. Nelle aziende continua a crescere soprattutto la pressione sui dati di accesso alla posta elettronica e in particolare sugli account di Office365. Si osservano anche sempre più tentativi di phishing effettuati sotto forma di catena di Sant'Antonio. Si viola un account di posta elettronica aziendale e in seguito si invia un'e-mail di phishing a nome della vittima a tutti i contatti che gli aggressori trovano nell'account violato. In questo modo si fa presto a mettere insieme migliaia di nominativi, soprattutto se il collaboratore o la collaboratrice in questione ha il contatto diretto con i clienti. Visto che in questi casi il mittente è noto al destinatario, c'è una maggiore probabilità che quest'ultimo creda alla storia e cada nella trappola del phishing. A quel punto il gioco ricomincia e vengono presi di mira i suoi contatti. Questo modus operandi è chiamato anche «chain phishing».

2.3.2 La rinascita del voice phishing

Il voice phishing continua a riguardare una piccola percentuale delle segnalazioni di phishing. Trattandosi tuttavia di telefonate molto mirate in cui il chiamante interagisce direttamente con la vittima, è probabile che le chance di successo siano di gran lunga maggiori. Questo è sicuramente un motivo per cui i phisher sono disposti a fare questo sforzo in più.

Verso la fine del 2023 si è registrato un boom di segnalazioni di chiamate da parte di sedicenti impiegati di banca, che facevano credere di voler bloccare un pagamento fraudolento. In alcuni casi il numero di telefono visualizzato corrispondeva persino a quello ufficiale della banca: si tratta in realtà di un numero che, attraverso la tecnica dello «spoofing», viene falsificato dai truffatori per farlo sembrare credibile. In molti casi, ad esempio, si affermava che vi fosse un addebito per l'acquisto di uno schermo piatto presso un negozio di elettronica. La voce all'altro capo della cornetta consigliava di telefonare immediatamente alla divisione antifrode della Polizia cantonale e comunicava altresì il numero da chiamare, anch'esso naturalmente riconducibile ai phisher.

Ciò che a prima vista può sembrare plausibile, in realtà è impossibile. Nel proprio sistema, infatti, la banca può visualizzare gli importi addebitati, ma non il prodotto o il servizio acquistato dal cliente. Quindi, generalmente una banca non può conoscere il tipo di acquisto effettuato da un cliente.

Solitamente gli aggressori si spacciano per impiegati di una grande banca, visto che la probabilità che la vittima vi abbia effettivamente un conto è statisticamente più alta. Ma i criminali hanno trovato un escamotage anche nell'eventualità in cui non riescano a indovinare correttamente la banca. Nel corso della telefonata cercano di scoprire quale sia l'istituto bancario della vittima e quindi richiamano poco tempo dopo, ma questa volta a nome della banca «giusta».

---

[26] Settimana 46: Phishing con presunta restituzione d'imposta e phishing di portafogli di criptovalute (ncsc.admin.ch);
Settimana 41: phishing di Microsoft 365 e FFS in diverse varianti (ncsc.admin.ch)

Come si evince dalle segnalazioni all'UFCS, gli aggressori utilizzano anche informazioni disponibili pubblicamente. In un caso, ad esempio, la vittima è stata contattata da un sedicente impiegato di banca che le ha chiesto se negli ultimi giorni avesse effettivamente predisposto un pagamento di una somma consistente. Stranamente il presunto destinatario era noto alla vittima per via di un'attività precedente. Da una ricerca su Internet ad opera dell'UFCS è risultato che sia il nome che il numero di telefono della vittima e del presunto destinatario erano comparsi in una presentazione pubblica che i due avevano effettuato insieme in passato. Questo dimostra che gli aggressori spulciano sistematicamente Internet alla ricerca di informazioni che possono poi sfruttare per attacchi di social engineering mirati. Ad oggi questo modus operandi era stato riscontrato soprattutto in relazione alla truffa del CEO, mentre ora pare si stia espandendo anche al fenomeno del voice phishing.

2.4 Segnalazioni di malware e hacking

2.4.1 Ransomware

Non per tutti i fenomeni si è osservato un aumento. Nella categoria ransomware, in particolare, i numeri hanno registrato un netto calo rispetto al 2022 fermandosi a quota 109, quasi 40 in meno rispetto all'anno precedente. La diminuzione ha riguardato soprattutto i privati, ma non le imprese. Nel 2023, infatti, sono state soltanto 11 le segnalazioni relative a privati, contro le 56 dell'anno precedente. I sistemi NAS (dispositivi di archiviazione collegati alla rete) nazionali presi di mira soprattutto nel caso dei privati vengono attaccati ancora solo sporadicamente – da un lato perché quest'anno non si sono registrate falle di sicurezza gravi, dall'altro perché gli attacchi probabilmente saranno anche stati troppo poco redditizi.

Se invece si osserva il numero di segnalazioni di ransomware ai danni delle imprese, il trend discendente è decisamente più moderato e il numero è praticamente stabile al livello dell'anno scorso – 98 contro 103 segnalazioni. Nel frattempo si nota come gli attacchi siano quasi sempre abbinati a una fuga di dati, il che incrementa ulteriormente l'entità del danno. Sul ransomware si veda anche il cap. 3.3.

Continua a essere particolarmente attivo il ransomware «LockBit». Altre famiglie di ransomware segnalate sono «Play», «MedusaLocker», «BlackCat/ALPHV», «Phobos», «BlackByte», «BlackBasta», «Babuk», «ECh0raix» e «Akira».

Raccomandazioni:

Sul sito dell'UFCS è disponibile un elenco di misure preventive per proteggersi dal ransomware e varie istruzioni operative su come procedere in caso di attacco.

2.4.2 Segnalazioni di hacking

Anche sul fronte dell'hacking si è registrato un aumento nel 2023. Rispetto al secondo semestre del 2022, nel periodo in esame le segnalazioni sono passate da 276 a 351. In questo caso sono soprattutto gli account dei social media a essere sotto pressione: in questa categoria l'NCSC ha ricevuto complessivamente 186 segnalazioni (+78). Gli aggressori si concentrano sempre più su account aziendali in cui è memorizzata una carta di credito. Una volta violato l'account, i criminali possono quindi attivare pubblicità – ad es. per offerte di dubbio contenuto

– a spese della vittima. Oltre al danno che si genera per la perdita dell'account social, quello finanziario può raggiungere svariate migliaia di franchi.

2.4.3 Alberghi nel mirino

A essere presi di mira, nella seconda metà del 2023, sono stati in particolare gli alberghi, i loro clienti e, in tale contesto, soprattutto la piattaforma booking.com. Già all'inizio dell'anno l'NCSC aveva avvisato di casi in cui un finto receptionist contattava gli ospiti degli alberghi per farsi comunicare i dati delle loro carte di credito.[27] Gli aggressori conoscevano tutti i dettagli della prenotazione e sfruttavano queste informazioni per convincere l'interlocutore che si trattasse veramente di una richiesta dell'hotel. All'epoca si sospettava che i cibercriminali fossero riusciti a infiltrarsi nell'account di «booking.com» dell'albergo.

Nel secondo semestre sono emerse ulteriori indicazioni circa il modus operandi utilizzato dagli aggressori per carpire le credenziali d'accesso a portali come booking.com. Nello specifico vengono utilizzati diversi metodi di ingegneria sociale per indurre il personale dell'albergo a cliccare su un link e installare un programma nocivo.

In una variante si fa credere che un ospite sia ricattato con immagini pornografiche che si presume siano state scattate nella camera dove soggiornava. Il mittente concede due giorni all'hotel per chiarire la questione e scoprire il colpevole, altrimenti sarà ritenuto complice. Quale prova dell'accaduto, l'intera documentazione del caso sarebbe stata archiviata in un file scaricabile tramite un link indicato nell'e-mail. Cliccando sul link, viene scaricato un malware che registra tutti i dati d'accesso disponibili e li trasmette ai truffatori, permettendo loro di visualizzare le prenotazioni attuali dell'albergo effettuate tramite piattaforme online come «booking.com».[28]

Oltre alle e-mail contenenti malware in allegato circolano anche vere e proprie e-mail di phishing rivolte direttamente al personale degli alberghi. Anche in questo caso si cerca di indurre le collaboratrici e i collaboratori in questione a rivelare i dati d'accesso a booking.com.

Raccomandazioni:

Soprattutto gli alberghi si trovano a dover aprire molti documenti trasmessi dagli ospiti. I file eseguibili non devono però essere aperti per nessuna ragione. Pensate a una strategia che permetta di tenere i computer destinati alla comunicazione con gli ospiti separati dal resto della rete (segmentazione della rete). Mantenete sempre aggiornati i sistemi.

27 Settimana 4: malware negli alberghi: dati delle prenotazioni utilizzati per truffare gli ospiti (ncsc.admin.ch)

28 Settimana 47: alberghi nel mirino dei cibercriminali (ncsc.admin.ch)

3 Situazione

3.1 Accesso iniziale con malware (trojan)

I trojan rientrano nella categoria dei malware che consentono di accedere al sistema di una vittima tramite l'inserimento di una cosiddetta «porta sul retro». Vengono spesso installati dopo aver ingannato gli utenti, ad esempio integrando il codice nocivo in un altro programma o nascondendolo in altro modo. Questo tipo di malware viene in genere diffuso via e-mail, o come allegato o tramite link. Anche il contesto dell'e-mail viene utilizzato per indurre l'utente a eseguire inconsapevolmente il codice nocivo. Per dare maggiore legittimità all'e-mail dannosa, alcuni aggressori si servono della precedente corrispondenza via mail che si sono procurati in modo illecito. Questo modus operandi è stato osservato soprattutto tra gli operatori di «Qakbot», un malware che, dopo la prima infezione, comportava sistematicamente attacchi ransomware. Nel secondo semestre del 2023, tuttavia, l'uso di «Qakbot» è calato drasticamente a seguito di un'operazione internazionale contro i sistemi infetti da «Qakbot» e le infrastrutture utilizzate dagli operatori del malware.[29] Nonostante la battuta d'arresto, tuttavia, i criminali che si nascondevano dietro le quinte di questi sistemi hanno corretto il tiro e continuato le loro attività. Dopo la distruzione di Qakbot si è assistito a un crescente numero di campagne finalizzate alla diffusione dei malware «PikaBot» e «DarkGate», che possiedono molte somiglianze con le attività di Qakbot, ad es. l'utilizzo della precedente corrispondenza via e-mail o l'uso di determinate infrastrutture identiche.[30] Si sono tuttavia aggiunti anche nuovi canali di diffusione, come ad es. l'utilizzo di software di messaggistica istantanea per uso professionale (tra cui «Microsoft Teams» o «Skype») o il ricorso alla tecnica del SEO poisoning (malvertising).[31]

Conclusione / raccomandazioni:

Non cliccate mai su link inviati con e-mail sospette e non aprite mai gli allegati. In caso di dubbio, chiedete al presunto mittente se ha effettivamente inviato l'e-mail in questione.

Quando cercate un software su Internet, prima di scaricarlo verificate di essere sul sito web del produttore o su un altro sito affidabile (ad es. una nota rivista di informatica).

Siate prudenti quando aprite una finestra di download.

Se possibile, impostate la funzione di aggiornamento automatico dei programmi. In alternativa, utilizzate sempre la funzione di aggiornamento integrata o scaricate la versione più recente direttamente dal produttore.

Non collegate mai al computer dispositivi USB sconosciuti o trovati casualmente.

---

29 Qakbot Malware Disrupted in International Cyber Takedown (justice.gov)

30 Settimana 42: Dynamite phishing: dopo Emotet e QakBot arriva DarkGate (ncsc.admin.ch);
Are DarkGate and PikaBot the New QakBot? (cofense.com)

31 PikaBot distributed via malicious search ads (malwarebytes.com);
Microsoft Teams used to deliver DarkGate Loader malware (malwarebytes.com)

3.2 Vulnerabilità: Ivanti CVE-2023-35078 e CVE-2023-35081

Ivanti è un fornitore di soluzioni di Unified Endpoint Management, di sicurezza Zero Trust e di Service Management, ossia offre alle imprese un sistema di controllo centrale con cui proteggere e manutenere i loro dispositivi. A livello globale sono in tutto oltre 40 000 le imprese che si affidano ai suoi prodotti.

Nell'estate del 2023, nell'Ivanti Endpoint Manager Mobile (EPMM) – noto in passato come MobileIron Core – è stata scoperta una vulnerabilità. Il 24 luglio 2023 il produttore ha informato i suoi clienti, mettendo a disposizione una patch da installare.[32] La falla di sicurezza è nota con il codice CVE-2023-35078 e riguarda tutte le release di prodotto supportate all'epoca, ossia 11.10, 11.9 e 11.8, oltre alle versioni precedenti non più supportate da tempo.

La falla di sicurezza critica, valutata con un punteggio CVSS[33] massimo di 10.0, consente a un aggressore non autenticato di accedere via Internet a determinati percorsi API[34] tramite i quali, in determinate circostanze, si riescono a visualizzare informazioni di identificazione personale (PII) come nomi, numeri di telefono e altri dettagli sui dispositivi mobili. Un utente malintenzionato potrebbe inoltre apportare modifiche alla configurazione e creare un account amministratore EPMM, il che gli offrirebbe ulteriori possibilità ancora più profonde di manipolare il sistema vulnerabile.

All'atto della pubblicazione dei dettagli sulla vulnerabilità, quest'ultima risultava già essere stata sfruttata, come spesso avviene in questi casi. Il 24 luglio 2023, ad esempio, l'autorità di sicurezza norvegese aveva informato la popolazione[35] di aver accertato l'uso della vulnerabilità per un attacco ai danni dei ministeri nazionali. Anche il produttore Ivanti cita nel suo advisory di essere a conoscenza di un numero limitato di clienti già caduti vittima di un tale attacco.

Mentre numerose imprese colpite erano ancora alle prese con l'eliminazione della CVE-2023-35078, qualche giorno dopo – il 28 luglio 2023 – con il codice CVE-2023-35081[36] veniva già resa nota la successiva falla di sicurezza nell'Ivanti Endpoint Manager Mobile (EPMM), identificata nel corso delle indagini sulla CVE-2023-35078. Anche in questo caso il produttore ha messo a disposizione informazioni e patch per colmare la falla di sicurezza.

La seconda falla è stata classificata con un punteggio CVSS di 7.2, quindi leggermente meno critica della precedente. Si tratta comunque di una vulnerabilità che consente a un ammini-

---

32 CVE-2023-35078 - New Ivanti EPMM Vulnerability (ivanti.com)

33 Il Common Vulnerability Scoring System (CVSS) è una norma tecnica aperta per valutare la gravità delle vulnerabilità di sicurezza di un sistema informatico. Si veda CVSS (wikipedia.org).

34 In un programma informatico, con application programming interface (API), in italiano «interfaccia di programmazione dell'applicazione», si indica un insieme di procedure (in genere raggruppate per strumenti specifici) atte a consentire la comunicazione tra diversi computer o tra diversi software o tra diversi componenti di software. Si veda Application programming interface (wikipedia.org).

35 Nulldagssårbarhet i Ivanti Endpoint Manager (MobileIron Core) - Nasjonal sikkerhetsmyndighet (nsm.no)

36 CVE-2023-35081 - Remote Arbitrary File Write (ivanti.com)

stratore autenticato di installare file dannosi su server ERMM (Arbitrary File Write). Se utilizzata in combinazione con la CVE-2023-35078, si possono aggirare del tutto l'autenticazione dell'amministratore e le restrizioni ACL[37].

Esattamente come per la prima vulnerabilità riscontrata, anche questa falla di sicurezza riguarda tutte le release di prodotto supportate al momento della pubblicazione, nonché le precedenti versioni non più supportate da tempo.

Il produttore Ivanti ha inoltre confermato sul proprio sito che, per la CVE-2023-35081, la complessità dell'attacco per un intruso è chiaramente ridotta, se sul sistema in questione il suo amministratore non ha ancora eliminato la prima vulnerabilità CVE-2023-35078.

L'NCSC ha avvisato attivamente i gestori di infrastrutture critiche e numerose altre imprese svizzere in merito alle due vulnerabilità. In base alle analisi tecniche condotte dall'NCSC si è provveduto a informare anche personalmente le possibili aziende colpite, fornendo loro consigli operativi concreti. Nonostante l'elevata criticità di entrambe le falle, il numero di vittime svizzere confermate è proporzionalmente ridotto.

Conclusione / raccomandazioni:

È assolutamente realistico che per lo stesso prodotto si rendano note pubblicamente più vulnerabilità gravi nell'arco di pochi giorni, come dimostra chiaramente il caso Ivanti. Il fattore tempo è un criterio di cruciale importanza nel Vulnerability Management. Le patch pubblicate andrebbero in ogni caso installate sui sistemi colpiti possibilmente senza perdite di tempo. I consigli del produttore vanno seguiti con la massima urgenza. Parallelamente, tuttavia, è fondamentale che ogni organizzazione e impresa conosca la propria infrastruttura e tenga un inventario aggiornato dei prodotti utilizzati.

La rapidità dell'intervento sulle lacune di sicurezza garantisce, da un lato, la sicurezza operativa dei sistemi informatici, riducendo allo stesso tempo anche la superficie d'attacco (attack surface) di un'impresa. Dall'altro, in determinati casi si può anche riuscire ad evitare che un aggressore approfitti del cosiddetto «Vulnerability Chaining». Concatenando tra loro più vulnerabilità, un intruso combina più falle di sicurezza esistenti per compromettere un sistema. Se un amministratore di sistema colma sistematicamente le falle di sicurezza attraverso un processo di Vulnerability e Patch Management, si complica il lavoro dell'aggressore e quindi si riducono anche le probabilità che l'attacco vada a buon fine.

3.3 Ransomware

3.3.1 Casi di ransomware

Nel semestre in esame vari attacchi di ransomware hanno colpito tra l'altro anche imprese che offrono soluzioni informatiche per le pubbliche amministrazioni e le PMI. Questi episodi sempre

[37] Una lista di controllo degli accessi (in lingua inglese access control list, abbreviato in ACL), in informatica, è un meccanismo usato per esprimere e/o definire delle condizioni che determinano l'accesso o meno ad alcune risorse di un sistema informatico da parte dei suoi utenti utilizzatori. Cfr. Lista di controllo degli accessi (wikipedia.org).

più frequenti ai danni della supply chain evidenziano quanto sia importante non solo adottare misure di prevenzione semplici, ma efficaci per proteggersi dai ciberattacchi, ma anche promuovere lo scambio di esperienze (a livello nazionale e internazionale) e comunicare in maniera competente sia durante che dopo un incidente.[38]

3.3.1.1 Una vulnerabilità nella catena di fornitura (supply chain)

Nel mese di novembre del 2023 l'operatore informatico Concevis AG, fornitore tra l'altro anche delle pubbliche amministrazioni, è stato vittima di un ransomware.[39] A seguito del ciberattacco, numerosi clienti hanno momentaneamente sospeso l'utilizzo dei servizi offerti da Concevis AG, onde evitare che i loro sistemi si infettassero attraverso le interfacce con la società.

Cresce inoltre l'interesse dei cibercriminali nei confronti delle catene di fornitura. Il gruppo del ransomware Everest, ad esempio, ha ricalibrato le proprie attività concentrandosi sul ruolo di Initial Access Broker. In altre parole, anziché sferrare loro stessi gli attacchi come fatto sinora, il gruppo si è specializzato nell'individuazione di «back door» all'interno dei sistemi delle organizzazioni e nella vendita di questi accessi ad altri cibercriminali. Secondo l'FBI[40] questa attività si basa sull'ottenimento di un accesso iniziale alle piattaforme informatiche delle vittime tramite terzi. Sfruttando le vulnerabilità degli accessi remoti controllati dal fornitore o da servizi di terzi, si utilizzano i tool di amministrazione dei sistemi legali per estendere i diritti all'interno dell'organizzazione prescelta.

Conclusione / raccomandazioni:

Anche gli attacchi e gli incidenti nelle supply chain possono mettere in ginocchio l'operatività di un'azienda e causare ingenti danni (successivi). È pertanto indispensabile affrontare il tema della cibersicurezza e della protezione dei dati con i propri partner, disciplinarlo a livello contrattuale e anche controllarlo.[41]

3.3.1.2 Backup offline e aggiornamenti periodici dei software

Nel mese di agosto del 2023 la rete del governo dello Sri Lanka, la Lanka Government Network (LGN), è stata vittima di un attacco ransomware che ha criptato i sistemi e i dati della LGN. Sebbene nell'arco di 12 ore si sia riusciti a ripristinare i sistemi, per alcuni dati l'operazione non è andata a buon fine. Non essendoci backup offline disponibili, si è dovuto ricorrere ai backup online, anch'essi tuttavia corrotti in seguito all'attacco. Le e-mail inviate e ricevute tra il 17 mag-

38 Si vedano anche le raccomandazioni dell'UFCS: Comunicazione in caso di attacco informatico (ncsc.admin.ch)

39 Attacco hacker alla società Concevis: interessata anche l'Amministrazione federale (ncsc.admin.ch)

40 FBI Private Industry Notification 231108.pdf (ic3.gov)

41 Supply chain security guidance (ncsc.gov.uk); ICT Supply Chain Resource Library (cisa.gov); Collaborazione con i fornitori di servizi informatici (ncsc.admin.ch)

gio e il 26 agosto 2023, ad esempio, non hanno più potuto essere ripristinate. L'attacco ransomware ha avuto successo anche perché nella LGN si utilizzavano ancora delle vecchie versioni di «Microsoft Exchange» (2013).[42]

Conclusione / raccomandazioni:

Effettuate regolarmente delle copie di sicurezza (backup) archiviando i vostri dati (anche) su un supporto esterno.[43]

Eseguite gli aggiornamenti di sicurezza al vostro software. Anticipate la fine del ciclo di vita di un software, sostituendolo per tempo.

3.3.1.3 Una comunicazione strutturata in fase di gestione dell'incidente è fondamentale

Nel mese di maggio del 2023 la società Unico Data AG, fornitore svizzero di soluzioni informatiche per PMI, è stata vittima di un attacco ransomware da parte del gruppo Play, a seguito del quale la maggior parte dei servizi dell'operatore era offline. L'impresa ha prontamente reagito all'attacco costituendo un'unità di crisi, incaricata di risolvere i problemi insorti, di segnalare l'incidente alle autorità competenti e di informare i clienti interessati. In seguito al rifiuto della società di pagare un riscatto, il gruppo del ransomware ha pubblicato i leak nel dark web. A distanza di qualche tempo l'amministratore delegato di Unico Data AG ha commentato pubblicamente l'accaduto, precisando le ripercussioni finanziarie dell'attacco e le risorse di tempo e di personale che erano state necessarie per la risoluzione del problema.[44] Nel parlare delle lezioni che l'azienda ha tratto dall'incidente, il CEO ha esortato le altre imprese a prepararsi ai ciberattacchi concentrandosi non solo sui piani di ripristino d'emergenza (disaster recovery), ma anche sulla comunicazione – interna ed esterna. In merito a quest'ultimo punto ha sottolineato l'importanza di stabilire quali informazioni comunicare nei rispettivi canali e da parte di chi.

Conclusione / raccomandazioni:

Attraverso una comunicazione strutturata e proattiva le vittime di un ciberattacco sono in grado di inquadrare l'accaduto e di informare in maniera obiettiva le loro collaboratrici e i loro collaboratori, i clienti, i partner, i media e la popolazione, evitando speculazioni.

Consigli dell'UFCS sulla Comunicazione in caso di attacco informatico (ncsc.admin.ch).

3.3.2 Monitoraggio delle varianti di ransomware e dei diversi attori

I gruppi di ransomware si adattano rapidamente al mutare delle circostanze, che si tratti di nuove vulnerabilità, di evoluzioni a livello tecnico o di personale sulla scena, di misure introdotte dalle autorità o di nuove prescrizioni giuridiche. Un esempio riguardante il primo caso è

---

42 Sri Lankan government loses months of data following ransomware attack (therecord.media); Crisis & Consequences: An Emerging Cyber Quandary for Sri Lanka (capsindia.org)

43 S-U-P-E-R.ch – Cosa tenere a mente quando si effettua il backup dei dati (ncsc.admin.ch)

44 «Der Cyberangriff hat uns insgesamt weit über 1 Million Franken gekostet» (inside-it.ch)

lo sfruttamento di una nuova vulnerabilità nel software «Confluence» di Atlassian, utilizzata per diffondere il ransomware «C3RB3R».[45]

3.3.2.1 Evoluzione degli attori e dei loro servizi

Nel corso del semestre in esame ci sono stati ancora mutamenti nei gruppi di ransomware e nelle loro azioni. I gruppi cambiano spesso composizione, nome e tipo di attività, a volte si fondono con altri gruppi o offrono loro i propri servizi, ad es. sotto forma di ransomware come servizio (Ransomware-as-a-Service, RaaS). Il mercato dei ransomware è fiorente come non mai, offrendo anche ad attori meno esperti la possibilità di sviluppare e adattare personalmente nuovi malware con facilità. È quanto accaduto ad esempio con il ransomware modulare «Lockbit 3.0», il cui codice ha iniziato a infiltrarsi nei sistemi nel settembre del 2023. I ricercatori di Kaspersky hanno trovato 396 sample diversi contenenti questo codice.[46] La presenza di numerose varianti di «Lockbit» complica il lavoro degli studiosi di cibersicurezza, il cui compito è attribuire gli attacchi ai rispettivi gruppi o individui e monitorarne le attività. Un'altra difficoltà è il boom di nuovi attori e varianti che si affacciano sulla scena dei ransomware.[47]

Il gruppo Royal, ad esempio, pare essere stato rimpiazzato dal gruppo BlackSuit. Potrebbe trattarsi di un semplice cambio di nome o marchio e/o di una variante derivante da quella precedente, visto che il malware «BlackSuit» possiede certe caratteristiche del codice simili a quelle di Royal.[48]

Il 2023 non ha visto soltanto la trasformazione di varianti esistenti, ma anche la nascita di nuove famiglie di ransomware che si presentano come innovative e uniche nel loro genere, come nel caso del RaaS «Rhysida». Quest'ultimo possiede un meccanismo di autodistruzione ed è compatibile con i sistemi operativi di Microsoft precedenti a Windows 10. Scritto nel linguaggio di programmazione C++, è stato compilato con lo strumento di programmazione «MinGW» e con librerie condivise (shared libraries). «Rhysida» è attivo da maggio 2023.[49]

3.3.2.2 Reazione a un'operazione di polizia

A fine 2023 l'FBI ha diretto un'azione internazionale contro il gruppo BlackCat/ALPHV,[50] sequestrando per svariati giorni il Data-Leak-Site (DLS) del gruppo. Le autorità di perseguimento penale sono riuscite a impadronirsi di 946 coppie di chiavi, con cui hanno avuto accesso alle comunicazioni criptate tra i malfattori e le vittime, ai siti dei leak e al panel degli affiliati del gruppo. In breve tempo, tuttavia, i cibercriminali hanno reso noto di aver attivato un nuovo DLS, su cui sono prontamente comparse sei presunte vittime. Da allora il gruppo del ransomware Lockbit sta cercando di reclutare affiliati e sviluppatori di BlackCat/ALPHV.

---

45 C3RB3R Ransomware | Ongoing Exploitation of CVE-2023-22518 Targets Unpatched Confluence Servers (sentinelone.com)

46 Leaked Lockbit ransomware builder analysis (securelist.com)

47 Orange Cyber Defense pubblica regolarmente un elenco delle diverse varianti di ransomware e dei rispettivi -attori: Map tracking ransomware, by OCD World Watch team (github.com)

48 Investigating BlackSuit Ransomware's Similarities to Royal (trendmicro.com); BlackSuit ransomware - what you need to know (tripwire.com)

49 Kaspersky crimeware report: GoPIX, Lumar, and Rhysida. (securelist.com)

50 Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant (doj.gov)

Al momento non esiste uno strumento di decrittazione universale per il ransomware «BlackCat/ALPHV». Attraverso le chiavi rese disponibili grazie all'intervento della polizia, alcune vittime possono tuttavia ripristinare i loro dati.

3.3.2.3 Adeguamento dei ricatti all'evoluzione del quadro normativo

I cibercriminali si adeguano anche a nuove prescrizioni e regolamenti, come ad esempio all'introduzione degli obblighi di segnalazione.

A questo proposito il nuovo gruppo RansomedVC utilizza una tattica di estorsione per cui mette in guardia le vittime dalla multa che saranno costrette a pagare, ai sensi della legislazione in materia di protezione dei dati (GDPR o altri testi normativi), se non pagheranno il riscatto richiesto e il caso diventerà pertanto di dominio pubblico. Il gruppo chiama la propria richiesta di riscatto «tassa per la pace digitale» (ingl. «Digital Peace Tax»), analogamente all'espressione utilizzata dalla gang del ransomware LockBit per identificare le sue operazioni – «servizio di Penetration Test con successivo pagamento».

3.3.2.4 Settori allettanti per i cibercriminali: energia e salute

I settori dell'energia e della salute sono bersagli prediletti dalle gang dei ransomware. Per via dei servizi erogati, infatti, entrambi tollerano tempi di guasto limitati. Nel caso delle aziende sanitarie si aggiunge il fatto che i servizi offerti ai pazienti sono indispensabili, se non addirittura vitali, e che la loro attività si basa sempre più su sistemi collegati in rete, fascicoli sanitari elettronici e telemedicina. Questa situazione può indurre i gestori di infrastrutture critiche a cedere rapidamente alle richieste di riscatto, pur di riavere l'accesso ai loro sistemi.

Negli incidenti che si sono verificati durante il secondo semestre del 2023 in ambito sanitario, le cure ai pazienti hanno potuto continuare a essere erogate perlopiù senza grosse limitazioni e le attività delle cliniche sono rimaste disponibili. Gli ospedali colpiti si sono tuttavia disconnessi per precauzione dal sistema delle cure mediche d'emergenza, con conseguente possibile reindirizzamento dei pazienti verso strutture vicine.

Per quanto riguarda gli incidenti che hanno colpito il settore dell'energia (incluse le centrali nucleari e gli istituti di ricerca), dal 2022 si osserva una ripresa degli attacchi di ransomware. In molti casi, per quanto abbia ripercussioni sui sistemi informatici e cripti i file, questo tipo di attacco non comporta perturbazioni alla produzione o distribuzione di energia, che pertanto può continuare a essere erogata senza interruzioni.

Raccomandazioni:

Sul sito dell'UFCS è disponibile un elenco di misure preventive per proteggersi dal ransomware e varie istruzioni operative su come procedere in caso di attacco.

3.4 Fughe di dati / gestione dei dati

I dati sono il nuovo oro nell'era dell'informazione. Le fughe di dati hanno conseguenze ad ampio raggio non solo per le organizzazioni direttamente interessate: le informazioni trafugate possono essere utilizzate per altri attacchi, per cui anche i privati possono finire nel mirino dei malfattori. I cibercriminali sono consapevoli di questa tendenza, tanto che i malware finalizzati

al furto dei dati (i cosiddetti Infostealer) e le piattaforme illegali di vendita dei dati stanno acquisendo sempre maggiore popolarità.[51] Nel mese di dicembre del 2023 sono finiti sotto i riflettori, in particolare, due grandi leak: in un caso, durante il periodo natalizio vari hacker hanno offerto gratuitamente sul dark web milioni di dati personali sensibili trafugati da ogni parte del mondo.[52] Nell'altro la società 23andme, che sviluppa test genetici per la ricerca genealogica, ha informato di una fuga di dati verificatasi ad ottobre 2023 che ha interessato i dati anagrafici e genetici di quasi sette milioni di clienti.[53] L'attacco ha sfruttato le password deboli e ripetute degli utenti, ottenute da precedenti fughe di dati, il che espone le vittime – in particolare – a un rischio più elevato di ulteriori attacchi, come sottrazioni di account, attacchi di phishing, furto d'identità o truffe finanziarie. Questi episodi risollevano la questione non solo della responsabilità delle organizzazioni nei confronti di un'adeguata protezione dei dati sensibili dei loro clienti, ma anche di quella dei singoli individui, che devono proteggere i loro account con misure di sicurezza forti. Occorre inoltre una maggiore consapevolezza dei dati che si vogliono condividere con le diverse organizzazioni.

Raccomandazioni:

Salvate soltanto i dati di cui avete realmente bisogno (economia dei dati) e cancellate quelli non più necessari oppure archiviate i dati da conservare ma non più utilizzati attivamente offline. Proteggete gli accessi ad account e dati con password forti e, se possibile, con l'autenticazione a più fattori (MFA).[54]

Nota:

Il 1° settembre 2023 è entrata in vigore, dopo la revisione totale, la nuova legge federale sulla protezione dei dati (LPD). Essa impone, tra i vari punti, la segnalazione all'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) in caso di violazione della sicurezza dei dati.[55]

3.4.1 Fughe di dati nel settore sanitario (internazionale)

Nel secondo semestre del 2023 è proseguito il trend delle grandi fughe di dati nel settore sanitario. A livello globale la sanità si posiziona al terzo posto per frequenza del fenomeno, soprattutto nei Paesi di lingua inglese. Anche in Europa le organizzazioni sanitarie sono nel mirino dei cibercriminali.

Essendo molti di essi mossi da intenti finanziari, la scelta concreta delle vittime è più che altro di natura opportunistica. Il settore della sanità è allettante soprattutto per gli hacker, fiduciosi del fatto che ospedali, assicurazioni malattie e operatori di servizi in tale ambito siano tendenzialmente propensi a pagare un riscatto piuttosto che vedere pubblicati questi dati particolar-

---

51 Cfr. studio di Trend Micro su dati e marketplace: Your Stolen Data for Sale (trendmicro.com)

52 Cybercriminals launched "Leaksmas" event in the Dark Web exposing massive volumes of leaked PII and compromised data (resecurity.com)

53 23andMe confirms hackers stole ancestry data on 6.9 million users (techcrunch.com)

54 Cfr. Proteggete i vostri account (ncsc.admin.ch)

55 DataBreach (edoeb.admin.ch)

mente degni di protezione – evitando così danni conseguenti quali la perdita di fiducia o strascichi legali dovuti alla violazione della privacy e della protezione dei dati. Le ripercussioni su clienti e pazienti possono rivelarsi anch'esse devastanti. Da un lato, il fatto di sapere che i propri dati sanitari possano essere consultati da persone non autorizzate è fonte di stress psicologico, oltretutto considerato il fatto che i dati trafugati possono essere utilizzati anche per ricattare gli stessi pazienti (cosiddetto «data extorsion»). Dall'altro, i dati sottratti consentono anche furti d'identità, frodi assicurative e altri reati o possono semplicemente essere rivenduti a terzi.

Gli attacchi si differenziano per complessità e forma: utilizzano diversi vettori, come ad esempio il phishing (cfr. cap. 2.3) e altre tecniche di social engineering[56], sfruttano vulnerabilità presenti nel software e in soluzioni cloud o colpiscono fornitori di servizi esterni. Gli attacchi alla supply chain, in particolare (cfr. capitolo 4.5.2 nel Rapporto semestrale 2023/1), hanno contribuito in maniera determinante all'aumento del numero di segnalazioni. Certe tendenze già descritte nel primo semestre del 2023, tra cui i data leak ad opera del gruppo Ci0p o gli attacchi a vari fornitori di software, sono proseguite anche nella seconda parte dell'anno.[57] Mentre certi attori a volte combinano il furto di dati con software di crittografia (ad esempio i gruppi Hunters International[58] e BlackCat/ALPHV), altri si concentrano sulla mera estrazione di dati, come il gruppo Karakurt. In passato alcuni cibercriminali affermavano di rinunciare esplicitamente ad attaccare le organizzazioni del settore sanitario per via del loro ruolo cruciale. Ma proprio i collettivi che vendono le loro competenze sotto forma di servizio (Ransomware-as-a-Service) e che attualmente sono tra gli attori più attivi – come il gruppo LockBit o BlackCat/ALPHV – si sono invece allontanati da questa posizione.[59]

Sebbene al momento gli istituti sanitari nazionali non siano specificatamente nel mirino dei cibercriminali, anche il settore svizzero della sanità non è immune da attacchi opportunistici. Un ciberattacco ai danni del fornitore di soluzioni sanitarie digitali Medgate ad agosto e uno successivo a settembre 2023, per quanto sventati con successo, hanno comunque comportato brevi interruzioni di servizio.[60] Nel mese di ottobre del 2023 un attacco ransomware all'istituto Psychiatrie Baselland ha causato un guasto tecnico ai sistemi per 12 giorni, ma l'incidente ha potuto essere risolto senza gravi conseguenze.[61] L'UFCS non ha informazioni circa eventuali fughe di dati avvenute nell'ambito di questi episodi.

---

56 Social Engineering – der Mensch als Schwachstelle (bsi.bund.de)

57 Lo sfruttamento massiccio di una vulnerabilità nel programma di scambio di file «MOVEit», iniziata a maggio 2023, ha sinora coinvolto i dati di circa 90 milioni di persone al mondo (stato: dicembre 2023), si veda Unpacking the MOVEit Breach: Statistics and Analysis (emsisoft.com).

58 Ad es. attacchi al centro tumori americano Fred Hutchinson e all'istituto sanitario Crystal Lake: Hunters International ransomware gang claims to have hacked the Fred Hutch cancer center (securityaffairs.com);
Ransomware gang claims to have stolen Crystal Lake Health Centers data (databreaches.net)

59 ALPHV ha tolto questa restrizione in un annuncio pubblicato nel dicembre del 2023 – pare a seguito delle misure repressive adottate dalle autorità di perseguimento penale americane: ALPHV/BlackCat Claims Healthcare Restrictions Removed for Affiliates (hipaajournal.com). Nel mese di dicembre del 2023 LockBit ha attaccato un ospedale pediatrico negli USA, contrariamente a quanto promesso in precedenza: Ransomware-Bande Lockbit wirft Skrupel über Bord (inside-it.ch)

60 Comunicato stampa: Cyberangriff auf Teile der IT-Infrastruktur von Medgate.pdf (medgate.ch)

61 Psychiatrie Baselland nimmt Normalbetrieb wieder auf - Psychiatrie Baselland (pbl.ch)

3.4.2 Fuga di dati nella città di Baden

Il 4 dicembre 2023 è stata pubblicata la notizia di una fuga di dati nella città di Baden, nel Canton Argovia.[62] Circa tre GB di dati della città sono stati resi disponibili per il download nel forum di hacker BreachForum. Da un'analisi approfondita è emerso che quanto trafugato conteneva informazioni come nomi, indirizzi, numeri di telefono, IBAN e fatture dei residenti, ma anche dettagli relativi agli investimenti effettuati dalla città di Baden.[63]

La città di Baden ha prontamente reagito incaricando dell'elaborazione del caso un team di esperti esterni, informando la popolazione con un comunicato stampa[64] e predisponendo un modulo di segnalazione[65] per chi fosse eventualmente interessato. Ha inoltre sporto denuncia alla polizia. Secondo quanto riferito dalla città di Baden, a metà ottobre 2023 i servizi informatici hanno registrato la presenza di ignoti che cercavano di accedere illecitamente ai server della tecnologia di informazione e comunicazione (TIC) delle città di Aarau e Baden. La falla di sicurezza sarebbe però stata immediatamente eliminata e si sarebbero adottate ulteriori misure di sicurezza. Considerata la tipologia di dati, si desume che i medesimi provengano da un sistema amministrativo interno in cui vengono gestite le fatture emesse e ricevute dalla città di Baden.[66] Non si è riscontrata una compromissione di altri sistemi.

L'episodio è un ottimo esempio di come si evolva un aggressore che cerca di affermarsi sulla scena criminale e acquisire credibilità. I dati sono stati inizialmente pubblicati su un forum di hacker da parte di una persona chiamata DragonForce. All'epoca quella persona non era ancora un utente assiduo del sito, ma si era registrata alla piattaforma soltanto qualche giorno prima. Anche il fatto che i dati fossero stati messi a disposizione gratuitamente è strano. Normalmente lo si fa soltanto come forma di ricatto in caso di mancata collaborazione della vittima (cfr. anche cap. 3.3) o se si tratta di hacktivisti in stile «hack and leak»[67]. La città di Baden non aveva tuttavia ricevuto alcuna richiesta di riscatto[68] e DragonForce non denunciava nemmeno particolari abusi. Molto lasciava a intendere che l'attore volesse farsi un nome sulla scena criminale, tanto più che a metà dicembre DragonForce aveva aperto un proprio data leak site nel dark web e tra i nomi illustri aveva nuovamente indicato la città di Baden, accanto ad altre presunte vittime. L'elenco di nomi internazionali evidenzia come l'attore stia agendo in maniera opportunistica e che le imprese o organizzazioni svizzere non sono di per sé il suo bersaglio principale.

Conclusione / raccomandazioni:

In linea di massima vale il principio: i dati sono preziosi. Vi è dunque anche un interesse criminale a impadronirsene e venderli con mezzi illeciti o a ricattare le vittime con la minaccia di pubblicare dati sensibili. Di conseguenza la discussione sul tema della sicurezza dei dati dovrebbe concentrarsi meno sul fatto *se* una fuga di dati possa verificarsi e dedicare maggiore attenzione alla domanda *quando* una tale fuga si verificherà e come i dati, nel caso estremo

62 Baden ist Opfer eines Hackerangriffs geworden (nzz.ch)
63 Hackerangriff auf Baden: Meldeformular eingerichtet (badenertagblatt.ch)
64 Comunicato stampa: IT-Sicherheit der Stadt Baden (baden.ch)
65 Meldestelle Datenexposition (baden.ch)
66 Stadt Baden: "Nur Rechnungsdaten betroffen" (inside-it.ch)
67 Cfr. Rapporto semestrale 2023/1 (ncsc.admin.ch), cap. 2.3
68 Comunicato stampa: IT-Sicherheit der Stadt Baden (baden.ch)

di una fuga, possano essere resi inutilizzabili per l'aggressore. Soprattutto dinanzi a cibercriminali estremamente sofisticati e competenti, è praticamente impossibile raggiungere un livello di protezione totale da un'eventuale fuga di dati. A incidere vi sono fattori difficilmente controllabili, come le vulnerabilità. È dunque fondamentale osservare i principi cardine della sicurezza e della gestione dei dati.

Ecco i **cinque principi** della conservazione dei dati: Stabilire **chi** archivia ed elabora **quali** dati, in **quale forma** e **dove** e **con chi** tali dati vengono condivisi. Questo significa, in particolare, che è più opportuno memorizzare i dati con un approccio conservativo: meno dati si salvano e meno dati devono essere protetti da accessi non autorizzati. I dati esistenti andrebbero inoltre controllati a cadenza periodica, cancellando quelli non più necessari. Va anche verificato se si possa effettuare un'archiviazione dei dati digitali offline.

A livello pratico, anche gli **aspetti tecnici** sono importanti: oltre alle classiche misure atte a garantire una «ciberigiene»[69] efficace, i dati andrebbero possibilmente salvati in forma codificata.

Sensibilizzazione: la consapevolezza della problematica da parte delle collaboratrici e dei collaboratori andrebbe affinata regolarmente. Ai fini della gestione e della protezione dei dati occorre stabilire, implementare e controllare processi chiari e attuabili. Infine, ognuno dovrebbe avere chiaro in mente che le informazioni in rete sono – volontariamente o involontariamente – a disposizione di tutti. I malintenzionati possono sfruttarle, utilizzandole per finalità di «social engineering». In caso di attacco, non lasciatevi mettere sotto pressione, mantenete la calma e rivolgetevi, se necessario, a specialisti del settore.

Verifica: i dati trafugati in passato possono essere riutilizzati per altri attacchi. Verificate periodicamente che le vostre credenziali d'accesso non siano comparse in un data leak, ad esempio sul sito Have I Been Pwned: Check if your email has been compromised in a data breach (haveibeenpwned.com) o su Identity Leak Checker des Hasso Plattner Instituts (hpi.de). Utilizzate possibilmente più siti di questo tipo. Se in uno di essi i vostri dati d'accesso non sono stati registrati come data leak, non è detto che non facciano parte di un altro data leak.

3.5 Sistemi di controllo industriali (ICS) e tecnologia operativa (OT)

Il collegamento in rete e la digitalizzazione di tutti gli ambiti della vita avanzano senza sosta e ovviamente non si limitano al mondo industriale. I controlli di processo basati sulla tecnologia operativa, integrati in procedure aziendali digitali, consentono non solo di incrementare significativamente l'efficienza, ma anche di godere di una maggiore flessibilità in fase di implementazione. Al contempo, tuttavia, questa interconnessione tra mondo fisico e digitale espone i sistemi aziendali ad attacchi di più ampia portata. Attori statali e, in misura sempre maggiore, anche gli hacktivisti attaccano sistemi di controllo industriali non sufficientemente protetti per manipolare i processi o fomentare l'incertezza tra le persone colpite. La maggiore minaccia per il funzionamento dei sistemi di controllo industriali, tuttavia, rimane quella degli attacchi

[69] Tra i punti cardine di una sana «ciberigiene» si annoverano ad esempio i seguenti temi: gestione delle password (ad es. hashing e salting), principio del privilegio minimo, segmentazione della rete e gestione delle patch e del ciclo di vita dei prodotti.

ransomware contro sistemi informatici attigui e non sufficientemente isolati, che possono compromettere almeno temporaneamente la continuità operativa dell'intera rete.

3.5.1 Gli attori statali evidenziano competenze più agili in ambito OT

Mentre gli attacchi missilistici contro le città ucraine e le infrastrutture critiche dominavano i reportage di guerra, il 10 ottobre 2022 il gruppo di hacker legato ai servizi di intelligence russi Sandworm sferrava un attacco di sabotaggio informatico contro un operatore della rete elettrica ucraina. Secondo il rapporto[70] pubblicato nel novembre del 2023 dall'azienda di cibersicurezza Mandiant, gli aggressori sono riusciti a infiltrarsi nell'infrastruttura su cui operava un controller microSCADA deputato al controllo degli ambienti OT (Operational Technology) delle sottocentrali dell'azienda elettrica. A quel punto l'accesso è stato utilizzato abusivamente per eseguire comandi di spegnimento delle sottocentrali. La particolarità di questo caso è la metodologia utilizzata, ossia il fatto di servirsi di funzionalità esistenti per sferrare l'attacco. Questo approccio «Living-of-the-Land (LOTL)» si osserva ormai da tempo in ambito informatico, ma ora sta prendendo piede anche nell'ambiente OT. Rispetto a un malware sviluppato personalmente[71], come quello utilizzato negli attacchi contro la rete elettrica della regione di Kiev nel 2016, questo procedimento consente una più rapida successione dall'accesso alla rete all'esecuzione del vero e proprio sabotaggio. Visto che i componenti sfruttati vengono impiegati anche in molti altri sistemi, questo modus operandi può essere adattato in modo più flessibile ad altri obiettivi.

Oltre alla rete elettrica, si sono osservati anche attacchi di sabotaggio informatico contro obiettivi dell'agricoltura ucraina, avvenuti contestualmente agli attacchi missilistici.[72]

3.5.2 Servizio di approvvigionamento idrico nel mirino degli hacktivisti

Nell'ambito dei conflitti internazionali come la guerra in Ucraina o l'escalation in Medio Oriente, gli hacktivisti non solo non si tirano indietro davanti ad attacchi alla disponibilità (DDoS) o alla pubblicazione di informazioni intercettate, ma non disdegnano neppure le manipolazioni di sabotaggio su dispositivi OT esposti (si veda anche cap. 3.6). Il gruppo di hacktivisti «CyberAv3ngers», ad esempio, ha iniziato ad attaccare l'infrastruttura del produttore israeliano Unitronics[73], perturbando i sistemi idrici e fognari almeno di Stati Uniti[74] e Irlanda[75]. Il gruppo, che si dice sia affiliato alle guardie della rivoluzione iraniane[76], sfrutta l'attenzione mediatica per diffondere il suo messaggio di propaganda anti-israeliana (si veda Fig. 4).

---

70 Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology (mandiant.com)

71 CrashOverride Malware (cisa.gov)

72 Russian influence and cyber operations adapt for long haul and exploit war fatigue (blogs.microsoft.com)

73 Exploitation of Unitronics PLCs used in Water and Wastewater Systems (cisa.gov)

74 Water Utility Control System Cyber Incident Advisory: ICS/SCADA Incident at Municipal Water Authority of Aliquippa (waterisac.org)

75 Two-day water outage in remote Irish region caused by pro-Iran hackers (therecord.media)

76 IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities (cisa.gov)

Fig. 4: Messaggio propagandistico su dispositivi compromessi.[77]

Il gruppo «Predatory Sparrow», invece, ha nuovamente colpito le stazioni di servizio[78] in Iran. Anche nell'ambito della guerra in Ucraina hacktivisti come il «Team OneFist» e il «People's Cyber Army of Russia» pubblicano ripetutamente sui loro canali social presunte documentazioni di attacchi contro sistemi di controllo industriali.

Conclusione / raccomandazioni:

Mettete al sicuro i vostri sistemi industriali onde evitare gli attacchi descritti in questo capitolo. A tale proposito l'UFCS propone alcune Misure di protezione dei sistemi di controllo industriali (ICS).

Lievemente più complessi sono gli standard minimi per diversi settori, che l'Ufficio federale per l'approvvigionamento economico del Paese UFAE ha definito in collaborazione con le rispettive organizzazioni di settore.

Per controllare che i propri dispositivi di sicurezza siano sufficienti a difendersi dalle attuali minacce in ambito industriale, è possibile fare riferimento all'Emb3d Framework di MITRE.

3.5.3 Dispositivi IoT utilizzati abusivamente come infrastruttura d'attacco

Ancora più frequente degli attacchi a processi controllati dall'OT o agli stessi dispositivi è il loro utilizzo improprio come infrastruttura d'attacco contro altri obiettivi. A essere particolarmente presi di mira sono i dispositivi (I)IoT[79], come router, videocamere ecc., non adeguatamente protetti o giunti al termine del loro ciclo di vita. Nel mese di novembre del 2023 il SektorCERT

77 Iranian Cyber Av3ngers Compromise Unitronics Systems (secureworks.com)

78 Iran petrol stations hit by cyberattack, oil minister says (reuters.com)

79 Internet delle cose (wikipedia.org); Industrial internet of things (wikipedia.org)

danese[80] ha pubblicato un'analisi su una serie di router Zyxel compromessi nel maggio del 2023, appartenenti ad alcuni suoi membri operanti nel settore dell'approvvigionamento energetico. È emerso che le vulnerabilità presenti in quei dispositivi erano state prontamente sfruttate da vari attori, ad esempio per integrare i router in botnet che a loro volta possono essere utilizzate abusivamente per sferrare attacchi DDoS contro altri obiettivi esposti sulla rete Internet, come i siti web. Anche in Svizzera sono stati compromessi diversi router di questi modelli. L'UFCS ha provveduto a informarne i gestori affinché potessero ripristinare i dispositivi.

Oltre a Zyxel, anche vecchi dispositivi Cisco e Netgear sono stati compromessi in altro modo per creare la KV-botnet[81], attribuita all'entità Volt Typhoon. Quest'ultima è associata ad attacchi di ricognizione compiuti contro infrastrutture critiche negli Stati Uniti.

Per fare in modo che in futuro diventi più difficile compromettere questi dispositivi, l'UE ha varato il regolamento sulla ciberresilienza[82], che introduce requisiti di cibersicurezza a livello di UE per la progettazione, lo sviluppo, la produzione e la messa a disposizione sul mercato di prodotti hardware e software. Il regolamento si applica a tutti i prodotti connessi direttamente o indirettamente a un altro dispositivo o a una rete.

Conclusione / raccomandazioni:

Al giorno d'oggi non sono solo i veri e propri dispositivi di rete, come i router, a essere connessi e costantemente online, ma anche molti altri apparecchi elettronici presenti nelle nostre case. Anch'essi devono essere protetti in maniera adeguata ed essere aggiornati nel momento in cui vengono rese note delle vulnerabilità.[83]

3.6 Il mondo ciber nei conflitti

L'ultimo rapporto semestrale, oltre a fornire una panoramica dei principali eventi accaduti nel ciberspazio nel contesto della guerra in Ucraina, aveva sottolineato come non vi fossero segnali di un calo delle attività da parte dei cibercriminali, quanto piuttosto un aumento del rischio di danni collaterali in relazione a gruppi di hacktivisti intenzionati a sferrare attacchi distruttivi.[84] Entrambe le previsioni si sono avverate, come dimostrano i principali sviluppi dei conflitti nella seconda metà del 2023.

3.6.1 Guerra in Ucraina

Nel contesto della guerra in Ucraina, le attività malevole nel ciberspazio sono continuate a ritmo crescente anche nella seconda metà del 2023. Il CERT ucraino, ad esempio, ha riferito di aver gestito nel 2023 ben 2543 incidenti, il 15 per cento in più rispetto al 2022, tra cui la

80 The-attack-against-Danish-critical-infrastructure.pdf (sektorcert.dk)

81 Routers Roasting on an Open Firewall: the KV-botnet Investigation (blog.lumen.com)

82 Regolamento sulla ciberresilienza: Consiglio e Parlamento raggiungono un accordo sui requisiti di sicurezza per i prodotti digitali (consilium.europa.eu)

83 Ciberdritta: le precauzioni da prendere con l'Internet delle cose (ncsc.admin.ch); Sicurezza nell'Internet delle cose (IoT) (ncsc.admin.ch)

84 Cfr. Rapporto semestrale 2023/1 (ncsc.admin.ch), cap. 4.7

diffusione di malware, phishing o anche la compromissione di account e sistemi.[85] Pubblica amministrazione, difesa, approvvigionamento energetico e telecomunicazioni sono tra i settori più bersagliati. L'Ucraina ha riferito anche di una crescente tendenza da parte della Russia a prendere di mira, con campagne di spionaggio, le autorità ucraine che indagano su possibili crimini di guerra russi. Il Paese ha inoltre registrato ripetuti tentativi d'attacco ai danni di obiettivi che erano già stati colpiti in passato.[86] Un nuovo modus operandi adottato dalle autorità ucraine è quello di rendere noti pubblicamente gli esiti delle cibercampagne: nel mese di novembre del 2023, ad esempio, il servizio di intelligence militare ucraino ha comunicato di essere entrato in possesso, attraverso una complessa operazione informatica, di numerosi documenti riservati dell'Agenzia federale russa per il trasporto aereo.[87] L'incidente più rilevante di questo periodo, tuttavia, ha riguardato l'Ucraina: il 12 dicembre 2023 Kyivstar è stato vittima di un ciberattacco. Kyivstar è il più grande operatore di telecomunicazioni dell'Ucraina e fornisce telefonia mobile e Internet a oltre la metà della popolazione nazionale. L'attacco ha causato interruzioni sia ai servizi erogati agli utenti di Kyivstar che a quelli ospitati sulla sua rete. Parte della popolazione, ad esempio, ha avuto un accesso limitato ai servizi finanziari, e la ricezione degli avvisi di raid aerei non era più garantita. Si è riusciti a ripristinare parzialmente i servizi la sera del 13 dicembre 2023, ma ci è voluta più di una settimana prima che tutti fossero nuovamente disponibili.[88] L'attacco è stato rivendicato dai gruppi di hacktivisti KillNet e Solnetspek. KillNet non ha fornito prove e già in passato si era vantato di attacchi, che tuttavia erano risultati non ad opera loro. Solnetspek, invece, ha pubblicato alcuni screenshot che testimoniano un accesso privilegiato ai sistemi di Kyivstar. Secondo l'Ucraina e diverse società di sicurezza informatica occidentali, il vero autore dell'attacco è Sandworm, un collettivo ritenuto affiliato all'intelligence militare russa che in passato aveva già preso di mira società di telecomunicazioni, e che ora sta utilizzando Solnetspek come copertura.[89] Secondo quanto riferito, l'incidente è stato una combinazione di attacchi DDoS e di malware per la cancellazione dei dati (i cosiddetti wiper). Solnetspek sostiene di aver «distrutto» oltre 10 000 stazioni e 4000 server di Kyivstar, compresi tutti gli archivi nel cloud e i sistemi di backup. Già nel marzo del 2023 c'erano stati i primi tentativi di penetrare i sistemi dell'organizzazione. A maggio 2023 gli aggressori sono finalmente riusciti a ottenere un primo accesso, compromettendo l'account di un collaboratore di Kyivstar e infiltrandosi nei sistemi.[90] Questo accesso non scoperto per mesi avrebbe tra l'altro consentito di carpire informazioni sui clienti, localizzare telefoni cellulari, intercettare SMS e compromettere anche account Internet protetti da un'autenticazione legata a un numero di cellulare, ad es. Telegram.

Per quanto riguarda la Svizzera, è estremamente improbabile che il Paese cada vittima di simili attacchi di sabotaggio da parte di attori statali. Non è escluso, tuttavia, che sia presa di mira da gruppi di hacktivisti coinvolti in un conflitto. Ne è un esempio NoName057(16), un

---

85 The CERT-UA Team has processed 2,543 cyber incidents over 2023 (cip.gov.ua)

86 How russian government-controlled hacking groups shift their tactics, objectives and capacities (cip.gov.ua)

87 Defence Intelligence of Ukraine conducted a cyber operation against Rosaviatsia (gur.gov.ua)

88 NetBlocks on X: Metrics show that connectivity on Ukraine telco Kyivstar is now largely restored (twitter.com); Russian hackers were inside Ukraine telecoms giant for months (reuters.com)

89 Hacker Group Linked to Russian Military Claims Credit for Cyberattack on Kyivstar (wired.com); Russia's Sandworm blamed for Kyivstar telecom cyberattack (theregister.com)

90 CEO of Ukraine's largest telecom operator describes Russian cyberattack that wiped thousands of computers (therecord.media); Exclusive: Russian hackers were inside Ukraine telecoms giant for months (reuters.com)

collettivo filorusso che, dopo le campagne di attacchi DDoS contro siti svizzeri del giugno 2023[91], nel secondo semestre del 2023 ha sferrato altri cinque attacchi DDoS ai danni di siti web nazionali, principalmente in risposta alle attività svizzere nell'ambito della guerra in Ucraina. Il 28 novembre – tre giorni dopo la visita del presidente della Confederazione in Ucraina – NoName057(16) ha infatti attaccato i siti web dell'Amministrazione federale e di organizzazioni operanti nel settore finanziario e del turismo. Pur avendo provocato solo danni marginali (non ci sono state restrizioni degne di nota nella disponibilità), gli attacchi di questi collettivi vengono utilizzati per scopi di propaganda.[92] A differenza delle campagne precedenti, NoName057(16) non attacca più i siti web di uno stesso Paese continuativamente per una settimana, ma cambia il suo obiettivo di giorno in giorno.

3.6.2 Conflitto in Medio Oriente

Dopo l'attacco di Hamas del 7 ottobre 2023 contro Israele, che ha portato a una nuova escalation di violenza nella regione, numerosi gruppi di hacktivisti hanno annunciato il loro coinvolgimento nel conflitto. Per molti versi, l'hacktivismo legato alla crisi in Medio Oriente è stato simile a quello della guerra in Ucraina. Gran parte dell'attività di questi gruppi, infatti, è mirata alla propaganda e/o alla disinformazione. Solo una minoranza di essi ha compiuto azioni nel ciberspazio che hanno avuto un impatto diretto sui sistemi informatici. Si è trattato principalmente di defacement di siti web e di attacchi DDoS, ma anche di azioni rivolte contro obiettivi al di fuori della zona di conflitto, perlopiù in risposta a dichiarazioni di sostegno per l'una o l'altra fazione.[93] Vari gruppi di hacktivisti, tuttavia, hanno condotto azioni più sofisticate e dannose. Il gruppo Cyber Toufan, ad esempio, avrebbe danneggiato oltre un centinaio di organizzazioni israeliane, pubblicando dati sensibili dopo aver compromesso la loro infrastruttura attraverso l'uso di wiper.[94] Il gruppo Karma si sarebbe anch'esso infiltrato in diverse organizzazioni israeliane per impiegare un wiper del tutto inedito, che possiede una versione per i sistemi Windows e una per i sistemi Linux.[95] Il gruppo Cyber Av3ngers, invece, ha preso di mira vari sistemi di controllo industriali di produzione israeliana, causando il defacement della loro interfaccia utente e rendendoli così inutilizzabili. I sistemi sono stati colpiti indipendentemente dalla loro posizione geografica, il che ha portato a incidenti in diversi Paesi al di fuori della zona di conflitto.[96] Alcuni di questi gruppi sono sospettati di fungere da copertura per attori statali, in particolare l'Iran, o di essere sostenuti da uno Stato.[97] La difficoltà di provare tali legami può essere sfruttata dai governi per negare la propria responsabilità e allo stesso tempo accrescere l'impatto mediatico delle loro azioni.

---

91 Si veda Rapporto semestrale 2023/1 (ncsc.admin.ch), cap. 2.1.
Rapporto di analisi dettagliata sugli attacchi DDoS «NoName057(16)» (ncsc.admin.ch)

92 Ukraine-Krieg: Russische Hackergruppe schürt in der Schweiz Verunsicherung (nzz.ch)

93 Hacktivist Involvement in Israel-Hamas War Reflects Possible Shift in Threat Actor Focus (securityscorecard.com)

94 Cyber Toufan goes Oprah mode, with free Linux system wipes of over 100 organisations (doublepulsar.com)

95 Mission "Data Destruction": A Large-scale Data-Wiping Campaign Targeting Israel (securityjoes.com)

96 Cfr. cap. 3.5.2

97 Iranian Hacktivist Proxies Escalate Activities Beyond Israel (checkpoint.com);
Iran surges cyber-enabled influence operations in support of Hamas (microsoft.com)

3.6.3 Sviluppi futuri

Non vi è nulla che faccia pensare che i ciberattacchi correlati al conflitto in Ucraina o in Medio Oriente possano diminuire. La tendenza che vede gruppi di hacktivisti – organizzati a livello puramente di società civile o utilizzati come copertura di uno Stato terzo – agire nel ciberspazio nel contesto di un conflitto sembra consolidarsi e affermarsi come nuovo standard. Nonostante, da quanto risulti ad oggi, questi gruppi non sembrino essere stati decisivi per nessuno dei protagonisti, le loro azioni potrebbero anche contribuire a trattenere forze statali nel ciberspazio e ad attirare la loro attenzione. Questi ulteriori «rumori di fondo», abbinati a una visione incompleta a causa del conflitto, fanno sì che sia complicato valutare la situazione.