11 maggio 2023 | Centro nazionale per la cibersicurezza NCSC

Rapporto semestrale 2022/II (luglio – dicembre)

Sicurezza delle informazioni

La situazione in Svizzera e a livello internazionale

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF
Centro nazionale per la cibersicurezza NCSC

1 Panoramica / Contenuto

Management summary

Tema principale: la cibersicurezza presso le PMI

La digitalizzazione avanza anche nelle PMI. Molti dispositivi informatici sono connessi fra loro tramite interfacce di rete. Processi come l'elaborazione degli ordini, la pianificazione, la produzione e la logistica sono sempre più interconnessi e vengono controllati digitalmente. Ciò aumenta il numero di sistemi accessibili via Internet, che devono quindi essere protetti nel miglior modo possibile. Tuttavia, spesso proprio le PMI non riservano alla cibersicurezza l'attenzione dovuta. Per questo motivo, il nuovo rapporto semestrale è incentrato sul tema della cibersicurezza presso le PMI e presenta gli aspetti più importanti in materia di protezione dalle ciberminacce.

La truffa rimane il tipo di incidente più segnalato

Nel secondo semestre del 2022 il numero di segnalazioni pervenute all'NCSC è rimasto molto elevato (17 341) ed è praticamente identico a quello del primo semestre del 2022. Lo scorso anno l'NCSC ha ricevuto complessivamente 34 527 segnalazioni, di cui l'85 per cento da privati, mentre il restante 15 per cento da imprese, associazioni e autorità. Le segnalazioni riguardano varie forme di truffa. Le e-mail minatorie inviate da presunte autorità di perseguimento penale, le cosiddette e-mail di «fake extortion», rappresentano quasi un terzo delle segnalazioni. Altri casi segnalati di frequente sono la truffa del CEO e la truffa mediante la manipolazione di una fattura.

Numero di ransomware invariato

Le segnalazioni relative a ransomware sono rimaste costanti e costituiscono quasi la metà di tutte le segnalazioni nella categoria riguardante i malware. Dei 76 casi segnalati, circa un terzo proviene da privati e due terzi da imprese. Il ransomware «Lockbit» prende di mira in modo particolare le imprese. Quest'ultimo è noto per la crittografia dei dati ma anche per il furto degli stessi, nonché per la loro pubblicazione online se non viene pagato il riscatto. Si tratta di una doppia estorsione che sta diventando sempre più comune. Poiché molte aziende hanno capito la minaccia dei ransomware e utilizzano la strategia di backup, la semplice crittografia non è più redditizia per gli aggressori. Spesso la prima infezione negli incidenti di ransomware è dovuta a una vulnerabilità o a una configurazione errata, oltre che a e-mail contenenti allegati o link dannosi.

Segnalazioni di hacking ancora in forte ascesa

Rispetto al primo semestre, nel secondo semestre il numero di hacking segnalati è quasi raddoppiato (276 segnalazioni). Gli account dei social media sono tra gli obiettivi preferiti dagli hacker, che ad esempio ricattano gli utenti o utilizzano gli account violati come mezzo pubblicitario per tentativi di truffe dell'investimento.

Editoriale

Spesso mi chiedono: «Le PMI sono meno sicure delle grandi imprese?». Per rispondere a questa domanda è necessario prima comprendere qual è la struttura di una tipica PMI. Un'impresa di mercato è considerata una PMI se impiega meno di 250 lavoratori. In Svizzera, il 99,7 per cento delle imprese rientra in questa categoria. La maggior parte degli occupati presso una PMI lavora nel settore della produzione di merci, nel commercio, nella manutenzione e nella riparazione di veicoli a motore e nel settore sociosanitario.

Ciò lascia già intendere che non esiste una tipica PMI e quindi neppure «la» cibersicurezza per le PMI per antonomasia. Come nel caso delle grandi imprese, le condizioni quadro nelle PMI per proteggersi dai ciberattacchi possono essere molto diverse. Ad esempio, un'impresa altamente tecnologica attiva nel settore farmaceutico deve soddisfare condizioni completamente differenti rispetto a un'impresa commerciale operante sul territorio regionale. Fattori significativi sono la disponibilità finanziaria, il livello di tecnologizzazione dell'impresa, il modello aziendale, la composizione dell'organico, la struttura e la cultura dell'impresa nonché il contesto economico e politico.

Perciò, rispondere alla domanda citata sopra è tutt'altro che facile. Tuttavia, nel presente rapporto semestrale, incentrato sulle PMI, emerge chiaramente che anch'esse sono bersagli di ciberattacchi. Potrebbero essere attacchi opportunistici non rivolti a target specifici o attacchi mirati a PMI che utilizzano in modo interessante i diritti della proprietà intellettuale.

Il presente rapporto semestrale intende evidenziare le vulnerabilità a cui sono esposte proprio le PMI e spiegare come possono essere protette, tenendo conto delle caratteristiche dell'impresa. Il compito dell'NCSC è creare le condizioni quadro volte a sostenere ulteriormente le PMI in Svizzera affinché possano proteggersi da sole. Vi invitiamo dunque a fornirci un riscontro sul rapporto e a condividere eventuali idee concernenti le PMI e i ciber-rischi.

Per quanto diverse siano tra loro, le PMI hanno una caratteristica che le accomuna: il numero spesso modesto di persone occupate non consente di istituire grandi reparti di sicurezza. Tuttavia, la cibersicurezza va affrontata in modo integrale e orientato all'attività aziendale. In ultima analisi ciò significa che sia la direzione di un'impresa sia i collaboratori necessitano di conoscenze di sicurezza informatica applicate nel loro settore di competenza. Se le PMI riescono a sviluppare tali conoscenze senza perdere forza economica, potrebbero presto ottenere un vantaggio non indifferente in un'economia sempre più digitale. Per poter sfruttare questa opportunità per la Svizzera quale Paese di PMI, è tuttavia fondamentale la collaborazione di autorità, rappresentanti del mondo economico e scientifico e società. Si tratta quindi di una sfida da affrontare insieme.

Florian Schütz, delegato federale alla cibersicurezza

2 Tema principale: la cibersicurezza presso le PMI

2.1 La digitalizzazione avanza

Quasi nessuno può sfuggire alla digitalizzazione. Per molte persone è impensabile una vita senza Internet. Nel frattempo i computer hanno fatto il loro ingresso in quasi tutti i settori dell'economia e della società, perlomeno nel settore terziario (comunicazione, amministrazione ecc.). Ma anche il settore secondario (produzione) spesso non può fare a meno del computer. Molti dispositivi informatici sono connessi fra loro tramite interfacce di rete e reti aziendali amministrative in una forma o nell'altra. Le operazioni riguardanti gli ordini, la pianificazione, la produzione, la logistica e la contabilità sono sempre più correlate ai processi parzialmente o completamente automatizzati.

Raccomandazioni

Siate avveduti: nella digitalizzazione occorre considerare non solo le opportunità e i vantaggi, ma anche le nuove dipendenze e i nuovi rischi. Pianificate sin dall'inizio la cibersicurezza in ogni fase della digitalizzazione.

2.2 Attività principale e strumenti di supporto

Per le imprese che offrono esclusivamente servizi digitali, la cibersicurezza dovrebbe essere una cosa ovvia: in fin dei conti possono lavorare soltanto se i loro sistemi funzionano in maniera corretta. Tuttavia, nella maggior parte delle imprese l'informatica viene impiegata principalmente come funzione di supporto. Viene data la priorità all'attività principale, che sia la fabbricazione di prodotti o l'erogazione di servizi. Finché i sistemi informatici funzionano, non vi si presta quasi attenzione. Se qualcosa non va come dovrebbe, spesso è comunque possibile organizzare una soluzione. Un guasto totale può tuttavia comportare conseguenze molto gravi: se non è più possibile pianificare né contabilizzare nulla, la logica conseguenza saranno interruzioni del lavoro e ritardi che eventualmente si riflettono sul bilancio. D'altro canto, anche la violazione del diritto della proprietà intellettuale (spionaggio industriale) o un pagamento eseguito erroneamente può causare danni ingenti sul piano finanziario.

Conclusione / raccomandazioni

I mezzi informatici sono strumenti di lavoro che necessitano di manutenzione e cura. Rivolgetevi a uno specialista per ottenere consulenza e supporto. Gli standard TIC minimi e gli standard TIC minimi per diversi settori definiti dall'Ufficio federale per l'approvvigionamento economico del Paese (UFAE), d'intesa con il mondo economico, fungono da raccomandazione e da guida.

2.3 Esercizio dei mezzi informatici e cibersicurezza

Nelle PMI, l'esercizio dei mezzi informatici aziendali include sovente anche la responsabilità per la cibersicurezza, che non di rado è considerata un'attività secondaria. Poiché la manutenzione dell'infrastruttura informatica è impegnativa, si rischia di trascurare la cibersicurezza.

Generalmente, solo le imprese che hanno certe dimensioni possono permettersi di assegnare alla cibersicurezza una funzione specifica. Mentre per quanto concerne le funzionalità informatiche sono stabiliti requisiti chiari e misurabili, la cibersicurezza fa parte della gestione dei rischi e deve quindi essere guidata dalla direzione. In particolare, è consigliabile riservare alla cibersicurezza una voce contabile a sé stante, in modo tale che le risorse siano disponibili esplicitamente per le corrispondenti misure.

Conclusione / raccomandazioni

Benché l'esercizio e la sicurezza delle infrastrutture informatiche siano correlati, appartengono a due ambiti d'intervento diversi. L'assegnazione di risorse a favore di misure in materia di cibersicurezza deve essere decisa nel quadro della gestione dei rischi.

2.4 Esternalizzazione dei fornitori di servizi

Gli uffici di tutte le imprese sono equipaggiati di computer, ma non tutte dispongono di una propria rete aziendale. Se tuttavia il lavoro deve essere svolto su più dispositivi, oggi è offerta la possibilità di esternalizzare la conservazione dei dati e di trasferire l'esercizio dei programmi sul cloud. Una siffatta esternalizzazione può essere sensata anche per alleggerire la rete aziendale o incrementare la flessibilità. Non da ultimo, i fornitori di servizi cloud dovrebbero disporre di buone conoscenze in materia di cibersicurezza, poiché erogano servizi informatici specializzati. Un'altra possibilità è ricorrere a un fornitore di servizi di cibersicurezza esterno che si occupi specificamente di tale ambito.

Conclusione / raccomandazioni

Se si stipulano contratti con fornitori di servizi esterni, bisogna tenere conto del fatto che anche la sicurezza va regolata di conseguenza. Oltre ad eventuali apposite misure in materia di protezione e difesa dai ciberattacchi (ad es. attacco DDoS, fuga di dati e ransomware), occorre trattare anche tematiche quali la protezione dei dati (backup) e gli obblighi di comunicazione in caso di ciberincidenti.

2.5 Prevenzione degli incidenti

Oltre alle misure tecniche di protezione, la formazione del personale in materia di ciber-rischi è una misura importante, perché i collaboratori rappresentano un elemento cruciale della catena di difesa. Anche se non è possibile garantire un rilevamento affidabile e autonomo delle e-mail nocive da parte dei collaboratori, la sensibilizzazione al pericolo è già di per sé uno strumento utile. Se, nel caso di un'e-mail sospetta o dubbia, i destinatari non eseguono direttamente ciò che è riportato nel messaggio, non cliccano sul link indicato o non aprono il file in allegato, bensì verificano l'e-mail internamente o chiedono al (presunto) mittente di confermare l'autenticità del messaggio, si riduce il rischio di riuscita di un ciberattacco.

Non si può mai escludere del tutto che succeda qualcosa, anche se la prevenzione e la sensibilizzazione sono ottimali. Per essere preparata a tali eventualità, l'impresa deve disporre di un piano per le emergenze. A tal fine, i processi e i livelli di escalation devono essere definiti e testati. Studiare in anticipo la strategia di comunicazione da adottare nelle situazioni di crisi,

sia interne che esterne, consente di allentare la pressione nelle emergenze, contribuisce a evitare errori e contribuisce così a sventare efficacemente un ciberattacco. Si raccomanda inoltre di stabilire contatti con eventuali fornitori di servizi che potrebbero intervenire in caso di incidente («incident response») in modo tale da non doverli cercare nel momento di bisogno.

Conclusione / raccomandazioni

La cibersicurezza non è tanto uno stato da raggiungere, quanto piuttosto un processo costituito da misure tecniche, organizzative e del personale che va curato.[1] In tale contesto, la formazione dei collaboratori è un punto essenziale.

Anche se si investe in modo considerevole nella prevenzione, un ciberincidente non si può mai escludere del tutto. Oltre ai piani per la gestione degli incidenti, è opportuno studiare in anticipo la strategia di comunicazione interna ed esterna.[2]

3 Contributi ospite: testimonianze su ciberattacchi

3.1 Ciberattacco all'azienda dei trasporti pubblici di Lucerna

Di Franz Theiler, capo Informatica presso Verkehrsbetriebe Luzern AG (VBL)

Nella notte di sabato 14 maggio 2022, l'azienda dei trasporti pubblici di Lucerna (VBL) ha subìto un ciberattacco mirato. Di prima mattina, i collaboratori del centro di coordinamento hanno informato il servizio di picchetto informatico riguardo a un guasto. Il reparto informatico è riuscito a individuare velocemente l'entità del danno, classificandolo come incidente straordinario. I sistemi informatici sono stati messi offline e la rete informatica della VBL è stata scollegata da Internet.

Il capo dell'unità Notfall und Krisenmanagement (NKM) ha convocato lo stato maggiore d'emergenza. Una volta accertati i fatti è stata informata la polizia di Lucerna e l'incidente è stato segnalato al Centro nazionale per la cibersicurezza (NCSC). Il mattino stesso, l'unità NKM e la direzione hanno comunicato il ciberattacco alle principali parti interessate quali le autorità, le imprese di trasporto e dei settori affini, i collaboratori e i media.

Già il sabato pomeriggio il team informatico della VBL e altri collaboratori del fornitore di servizi informatici esterno si sono riuniti presso la sede della VBL per coordinare e avviare i lavori. Il reparto di informatica della VBL gestisce i sistemi dei trasporti pubblici critici sotto il profilo dell'esercizio e ad alta disponibilità per clienti interni ed esterni in tutta la Svizzera. Si tratta di un sistema TIC molto complesso che funziona negli ambienti Windows e Linux. Grazie a una reazione tempestiva volta a contenere e ad analizzare la crisi, è stato possibile individuare ed eliminare il malware nonché a ricreare e a isolare i sistemi di base necessari. Tramite l'ultimo backup i sistemi sono stati ripristinati passo dopo passo, esaminati e integrati in ambiente produttivo mediante un processo controllato e consolidato. L'impeccabile interazione tra collaboratori, fornitori e specialisti ha permesso di contenere rapidamente la crisi e di effettuare un

1 Promemoria sulla sicurezza delle informazioni per le PMI (ncsc.admin.ch)
2 Incidente – Cosa fare? (ncsc.admin.ch)

ripristino efficace. Le autorità competenti di Lucerna hanno svolto le indagini forensi. Nel processo di ripristino, la sicurezza dei sistemi è stata aumentata in modo selettivo attraverso misure mirate.

I passeggeri non hanno risentito in alcun modo del ciberattacco. Per motivi di sicurezza sono stati disattivati soltanto i monitor delle partenze. A posteriori si può affermare che la VBL era ben preparata alla situazione di crisi. I settori operativi sono sempre stati in grado di garantire l'esercizio in modo organizzato, sebbene in forma limitata. Per alcune settimane il team interno preposto alla gestione di emergenze e crisi si è riunito quotidianamente, riferendo anche alla direzione, la quale ha svolto una funzione di ponte con le divisioni specializzate.

L'NCSC ha fornito supporto alla VBL in questa difficile situazione in modo tempestivo e orientato al cliente. Le informazioni ricevute hanno consentito alla VBL di ottenere spiegazioni preziose e certe in merito ai truffatori e al loro modo di agire. Ringraziamo anche l'NCSC per le due interessanti presentazioni che ha tenuto durante l'evento informativo per quadri e collaboratori. In tale occasione ha saputo infatti sensibilizzare con grande passione ed entusiasmo i collaboratori della VBL sul tema dei ciberattacchi. In quanto gestore di trasporti pubblici con infrastrutture critiche, la VBL può partecipare agli incontri organizzati dall'NCSC. Beneficia così di un regolare scambio di informazioni e apprende le novità nel settore della sicurezza informatica.

3.2 Un attacco ransomware spiegato dalla polizia

Sezione Criminalità digitale, polizia cantonale di Berna

I ransomware sono virus informatici che rendono inaccessibili i file dei computer infettati e chiedono il pagamento di un riscatto, in genere in criptovalute, per ripristinarli. Un attacco ransomware è automatizzato e viene compiuto da un gruppo organizzato di criminali. Se l'impresa vittima dell'attacco non intende rispondere alla richiesta di riscatto, gli aggressori minacciano di divulgare informazioni sensibili di clienti o di venderle sul dark web. Così facendo, viene lesa anche la reputazione dell'impresa.

Nel caso in questione, l'impresa ha segnalato il ciberattacco al centralino della polizia cantonale di Berna, che ha poi trasmesso la segnalazione alla sezione Criminalità digitale competente. In seguito, questa sezione ha nominato un team di investigatori e ha convocato gli esperti del settore specializzato Analisi forense digitale al fine di pianificare le prime misure. Un caso di ransomware richiede sempre la collaborazione interdisciplinare tra diversi attori. Come nel caso qui presentato, l'interazione con l'impresa colpita è di fondamentale importanza per rilevare informazioni utili e individuare il piano d'azione. Una buona cooperazione è determinante sotto vari aspetti perché, quando si verificano attacchi ransomware, l'impresa non si focalizza sulle rilevazioni e sulle indagini, bensì sulla ricostruzione dei dati e sulla ripresa dell'attività.

Nella fattispecie, oltre alla polizia era stato subito contattato anche un fornitore di servizi di sicurezza privato per aiutare a ripristinare l'infrastruttura. La collaborazione con quest'ultimo è stata proficua. Tuttavia ciò dipende dall'impresa coinvolta, in particolare da quanto è disposta a contribuire alle indagini e dalle sue priorità.

Visto che un attacco ransomware è tecnicamente complesso, sono necessari colloqui e riunioni per affrontare le vulnerabilità che hanno permesso l'accesso indebito.

Oltre alle indagini, l'impresa interessata si attendeva dall'NCSC consigli su come procedere e in particolare informazioni legali, dal momento che un simile attacco può fare emergere altre parti lese e colpire dati sensibili.

Nel caso presentato l'impresa ha reagito in modo esemplare, segnalando l'attacco il prima possibile alla polizia e ricorrendo a un fornitore di servizi di sicurezza privato. Questo ha permesso il corretto funzionamento delle procedure tra gli esperti della sezione Criminalità digitale e gli esperti del settore specializzato Analisi forense digitale. Si sconsiglia comunque di prendere in considerazione il pagamento di un riscatto, perché contribuirebbe a finanziare la criminalità organizzata. La propensione a pagare da parte della vittima dipende spesso dal livello di crittografia dei dati, dalla probabilità di poterli ripristinare e, non da ultimo, dall'ammontare del riscatto. Nel presente caso, l'impresa ha agito in modo esemplare e non ha mai preso in considerazione il pagamento di un riscatto. Per evitare di trovarsi in una situazione simile, è consigliabile sensibilizzare i collaboratori sui rischi legati al ciberspazio e a investire in corsi di formazione nonché in un'infrastruttura sicura. L'impresa vittima di ciberattacco ha potuto riprendere la propria attività dopo poco tempo, anche se la completa risoluzione dell'incidente ha richiesto qualche settimana.

4 Segnalazioni provenienti da imprese e privati

4.1 Segnalazioni di ciberincidenti – Panoramica

Anche quest'anno il numero complessivo di segnalazioni è nettamente aumentato. Con un totale di 34 527 segnalazioni, la cifra non è raddoppiata rispetto all'anno precedente (21 714 segnalazioni) ma, in termini assoluti,12 813 segnalazioni rappresentano un numero comunque più elevato rispetto all'anno scorso (incremento nel 2020/2021: +10 881). Da un lato, ciò è da attribuire alla crescente popolarità dell'NCSC e al suo modulo di segnalazione; dall'altro, il nuovo aumento è riconducibile anche ad altri motivi, soprattutto all'incremento delle segnalazioni di finte e-mail minatorie a nome della polizia (cfr. n. 4.2.1) e di «spoofing», la tecnica che permette di visualizzare un numero di mittente fasullo (cfr. n. 4.5.1). Il fatto che nel secondo semestre del 2022, con un totale di 17 341 segnalazioni, sia pervenuto praticamente lo stesso numero di segnalazioni del primo semestre indica che in futuro tale cifra non aumenterà più nella stessa misura degli ultimi tre anni.

L'85 per cento delle segnalazioni è giunto da privati, mentre il restante 15 per cento da imprese, associazioni e autorità. I casi più frequenti segnalati dalle imprese riguardano la truffa del CEO (190 segnalazioni nel secondo semestre del 2022), il «business e-mail compromise», in cui la vittima viene truffata mediante la manipolazione di una fattura (45 segnalazioni), gli attacchi ransomware (54 segnalazioni) e gli attacchi alla disponibilità («distributed denial of service », DDoS; 13 segnalazioni). Inoltre, sono stati registrati tentativi di estorsione («fake extortion») che hanno preso di mira privati, ma non solo. Esistono varianti di attacchi che puntano direttamente alle imprese, ad esempio i tentativi di «fake extortion» contro gli amministratori web descritti al numero 4.4.2. Anche i tentativi di phishing non sono più rivolti unicamente ai privati bensì, con sempre maggiore frequenza, anche ai collaboratori delle aziende. A essere nel mirino sono soprattutto i dati di accesso a Microsoft Office 365, come spiegato al numero 4.3.2.

Segnalazioni settimanali pervenute all'NCSC nel secondo semestre del 2022

Fig. 1: Segnalazioni settimanali pervenute all'NCSC nel periodo luglio–dicembre 2022, cfr. anche Numeri attuali (ncsc.admin.ch).

Segnalazioni pervenute all'NCSC nel secondo semestre del 2022 per categoria

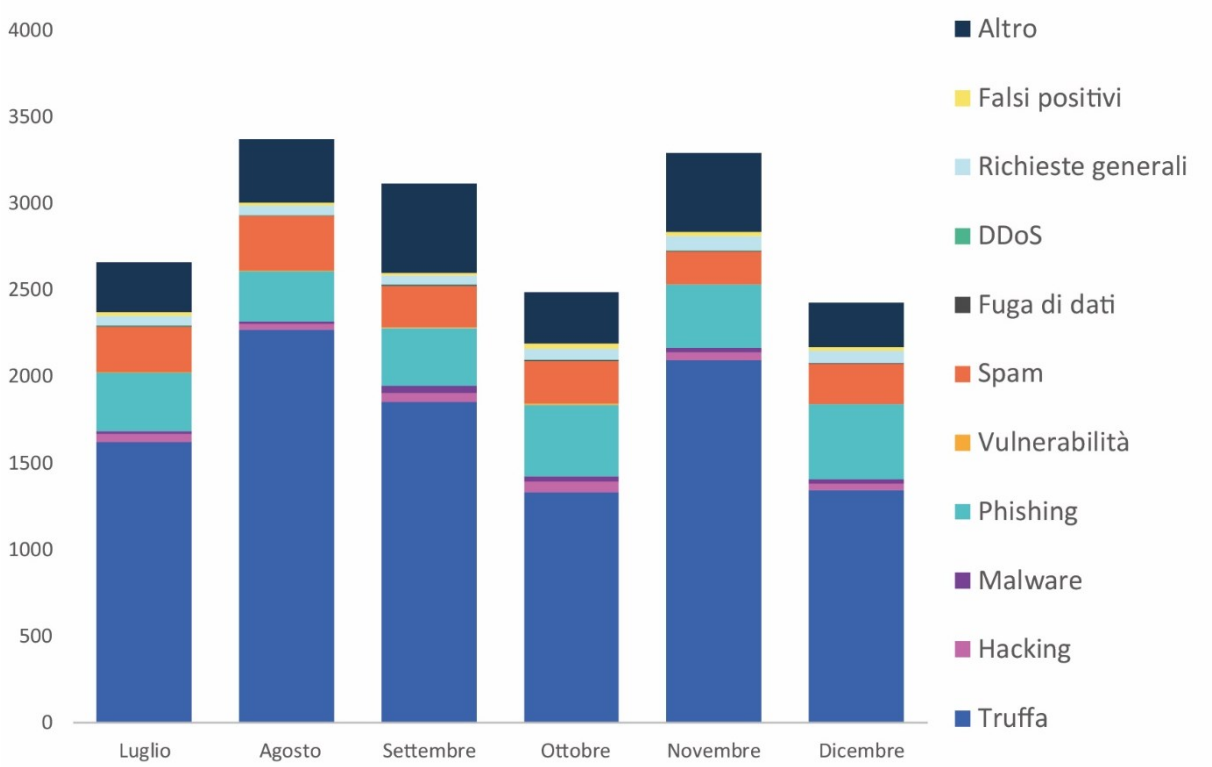

Fig. 2: Segnalazioni pervenute all'NCSC nel secondo semestre del 2022 per categoria, cfr. anche Numeri attuali (ncsc.admin.ch).

4.2 La truffa rimane il tipo di incidente più segnalato

4.2.1 Diverse varianti di e-mail minatorie inviate a nome della polizia

Nel secondo semestre del 2022 sono pervenute 5179 segnalazioni di e-mail minatorie fasulle inviate da presunte autorità di perseguimento penale. Questo è risultato essere il fenomeno più diffuso tra i ciberattacchi. Non sorprende quindi che anche nella settimana record 36, nella quale è stato registrato il numero più alto di segnalazioni del 2022 (954), le presunte e-mail minatorie a nome della polizia abbiano rappresentato la quota maggiore, con un totale di 418 segnalazioni. In queste e-mail minatorie le vittime sono accusate di un grave reato (di solito connesso alla pedopornografia). Vi viene loro comunicato che possono sottrarsi a un'azione penale soltanto se pagano una certa somma di denaro. Nel 2022 l'NCSC ha ricevuto oltre 11 051 segnalazioni che rientrano in questa categoria, 5179 delle quali nel secondo semestre, ossia circa un terzo del totale.

Fig. 3: Diverse varianti di false e-mail minatorie a nome delle autorità di perseguimento penale con mittenti e loghi assemblati a caso. Ultima figura a destra: i truffatori utilizzano abusivamente il nome dell'NCSC, ma con il logo sbagliato.

Per conferire alle e-mail minatorie un aspetto ufficiale, i truffatori assemblano in modo più o meno casuale il nome e il logo di diverse autorità di perseguimento penale svizzere ed estere. Nel secondo semestre del 2022, ad esempio, sono stati utilizzati abusivamente come mittenti i nomi delle autorità di polizia cantonale dei Cantoni del Vallese, di Vaud e di Ginevra. Tra le autorità estere, hanno riscontrato l'uso indebito del proprio nome l'Europol e l'Interpol, nonché la polizia francese, belga e olandese. Anche l'NCSC non è stato risparmiato: il suo nome figurava come mittente di queste mail minatorie. Gli aggressori hanno tuttavia commesso un errore, perché hanno utilizzato il logo dell'omonima autorità britannica responsabile della cibersicurezza. Il metodo più diffuso rimane l'e-mail fittizia in cui l'Ufficio federale di polizia (fedpol) risulta essere il mittente. I documenti allegati riportano la firma finta della direttrice di fedpol Nicoletta della Valle o della consigliera federale Karin Keller-Sutter, ex capo del Dipartimento federale di giustizia e polizia.

4.2.2 Amministratori web nel mirino

Nel secondo semestre del 2022 sono stati riscontrati casi di falsa estorsione anche contro amministratori web. Complessivamente l'NCSC ha ricevuto 114 segnalazioni di questo tipo. Nella lettera di estorsione, inviata solitamente mediante il modulo di contatto presente sul sito web o via e-mail, si comunica che la pagina è stata oggetto di un attacco di hacker e che la base dei dati di riferimento è stata rubata. Gli hacker minacciano infine di rendere pubblici tali dati. Tutte le richieste presentano una formulazione e una struttura simili, come nelle e-mail di «fake sextortion». Spesso la caratteristica di queste estorsioni è l'utilizzo degli stessi indirizzi bitcoin delle e-mail inviate alle aziende. Se qualcuno pagasse il riscatto, gli aggressori non riuscirebbero nemmeno a risalire alla persona che lo ha pagato. Si tratta quindi di un vero e proprio bluff.

Nel periodo in esame è stata riscontrata per la prima volta una nuova sottovariante di questo tipo di truffa: alcuni responsabili della sicurezza sono stati contattati da sedicenti ricercatori in merito a presunte vulnerabilità del sistema. Tuttavia, nella parte conclusiva dell'e-mail si indicava che, nel quadro della procedura di «responsible disclosure», per le vulnerabilità era prevista un'apposita ricompensa. In realtà, la vulnerabilità consisteva solo nella mancata attivazione della funzione «HTTP strict transport security» (HSTS)[3] e non vi era alcuna falla di sicurezza concreta. Anche se raccomandiamo vivamente di implementare il criterio di sicurezza HSTS, la sua assenza non può essere considerata una classica vulnerabilità. In rete si trovano numerose pagine che consentono anche a persone prive di conoscenze informatiche particolari di verificare la presenza nei siti web dei comuni elementi di sicurezza. Gli aggressori sfruttano queste pagine facendo leva sull'insicurezza degli amministratori web, con la speranza di ottenere una ricompensa.

[3] Se la funzione HSTS è attivata per un sito web, nel protocollo HTTPS viene utilizzato un header supplementare che impone al browser di usare esclusivamente connessioni sicure dalla prima apertura del sito.

Hi Team,I am a security researcher and found a vulnerability on your website.

Vulnerability : Non - secure requests are not automatically upgraded to HTTPS | HSTS missing

I am hoping to receive a reward for the responsible disclosure of vulnerability.

Looking forward to hearing from you soon.
Kind Regards,

Fig. 4: E-mail riguardante una presunta lacuna di sicurezza del server web con richiesta di ricompensa.

4.2.3 Truffa dell'investimento

Con 219 segnalazioni pervenute all'NCSC e un danno complessivo di oltre 4 milioni di franchi, anche nel secondo semestre del 2022 i casi di truffa dell'investimento rientrano fra i reati che causano le perdite finanziarie più ingenti. Si tratta soltanto degli importi citati dagli autori delle segnalazioni inviate. Dal momento che non tutti i casi vengono segnalati all'NCSC e che presumibilmente un gran numero di casi non è stato segnalato, l'importo effettivo dei danni potrebbe essere ben più elevato. Le vittime vengono adescate con vari tranelli e poi indotte a investire il loro denaro su siti sospetti. La tecnica più conosciuta consiste in promesse pubblicitarie fittizie, nelle quali personalità note raccontano come guadagnare molti soldi velocemente. Qualche anno fa circolavano interviste false a Roger Federer, seguite da pagine pubblicitarie ingannevoli che facevano riferimento al programma televisivo «Höhle der Löwen». Attualmente per questo tipo di pubblicità vengono spesso utilizzati in modo illecito anche i nomi dei consiglieri federali. Nel secondo semestre l'NCSC ha ricevuto 469 segnalazioni di pubblicità fraudolenta che promette guadagni facili e veloci. Tuttavia, le segnalazioni di questo tipo sono leggermente diminuite rispetto al semestre precedente (619 segnalazioni). Benché l'NCSC riceva segnalazioni da parte di vittime che sono cadute in questa trappola della pubblicità, il numero di truffe riuscito è probabilmente esiguo. Pertanto, gli aggressori ricorrono viepiù ad altri stratagemmi per convincere le vittime a investire il loro denaro. Un metodo frequentemente osservato consiste nell'instaurare un contatto all'apparenza innocuo sui social media o sui siti di incontri. Gli aggressori investono molto tempo per conquistare la fiducia della vittima per poi convincerla in un secondo momento a fare un investimento all'apparenza redditizio. I truffatori condividono inoltre la loro esperienza affermando di essere diventati ricchi grazie a questi investimenti.

4.3 Segnalazioni riguardanti tentativi di phishing

Nel secondo semestre del 2022 l'NCSC ha ricevuto 2177 segnalazioni riguardanti tentativi di phishing che sono pervenute sul suo portale di segnalazione. Il numero è leggermente diminuito rispetto al semestre precedente (2544 segnalazioni). I casi di phishing tramite e-mail che prendono di mira le carte di credito sono ancora preponderanti. Spesso però gli aggressori si impossessano anche di altri dati, come le credenziali di accesso delle e-mail. Nello specifico, gli account di posta elettronica aziendali rappresentano un grande valore per i truffatori, come descritto al numero 4.3.2. Tuttavia anche gli account di posta elettronica privati sono un bersaglio allettante. L'account di posta elettronica è diventato la chiave di accesso a tutti i negozi

e i servizi online. Se si dimentica la password di un fornitore di servizi Internet, nella maggior parte dei casi è possibile reimpostarla tramite l'account di posta elettronica. Ciò significa che i cibercriminali possono accedere a numerosi account se riescono a impossessarsi della password dell'indirizzo e-mail della vittima. Se l'account di un negozio online viene violato è possibile accaparrarsi l'accesso a beni e servizi. Nel frattempo i truffatori hanno imparato a utilizzare le credenziali violate di e-mail e social media anche per avvalorare i loro tentativi di falsa estorsione (cfr. n. 4.4.2).

Pagine di phishing per settimana

Fig. 5: URL di phishing verificati e confermati dall'NCSC per settimana nel secondo semestre del 2022.
I dati attuali sono disponibili su: https://www.govcert.admin.ch/statistics/phishing/.

4.3.1 I truffatori sfruttano il calcolo della probabilità

E-mail che annunciano presunte fatture di Swisscom o Sunrise pagate due volte, messaggi SMS concernenti rimborsi fasulli di biglietti delle Ferrovie federali svizzere (FFS) o consegne fittizie di pacchi. Tutte queste notifiche hanno un punto in comune, ossia la probabilità relativamente alta che la storia inventata dagli aggressori appaia plausibile alla vittima. Ad esempio, molte persone sono in attesa di un pacco, pagano i servizi forniti da Sunrise o Swisscom mediante addebito diretto o hanno realmente presentato una richiesta di rimborso alle FFS. In questi casi, gli aggressori sfruttano a loro favore il calcolo della probabilità e inventano la loro storia basandosi su pratiche comuni che i cittadini svolgono di frequente. L'invio di messaggi che annunciano la presunta consegna di pacchi è un classico esempio. I truffatori inducono le vittime ad aprire una pagina dove vengono invitate a inserire i dati della carta di credito. Quasi un quarto dei casi di phishing (532 segnalazioni) è dovuto a notifiche fraudolente riguardanti la consegna di pacchi. Poiché dopo la pandemia di COVID-19 gli acquisti online sono aumentati in modo esponenziale, la probabilità che qualcuno stia effettivamente aspettando un pacco è alta. Ipotizzando che il 10 per cento della popolazione faccia un acquisto online alla settimana, se gli aggressori inviano settimanalmente 100 000 e-mail, la probabilità che qualcuno stia realmente aspettando un pacco riguarda circa 10 000 persone. Lo stesso principio si applica anche ai tentativi di phishing con il pretesto di una presunta fattura di Swisscom pagata

due volte. Se le e-mail che annunciano il presunto doppio pagamento a Swisscom o Sunrise vengono inviate a persone con indirizzi di posta elettronica «bluewin.ch» o «sunrise.ch», la probabilità che la storia inventata sia credibile e che i destinatari cadano nel tranello è elevata. Alla fine del 2022, i truffatori si sono concentrati sui rimborsi fasulli di biglietti delle FFS. Anche qui il pretesto dei truffatori è molto verosimile. Infatti in molte segnalazioni pervenuteci, le vittime affermano di aver atteso effettivamente un rimborso da parte delle FFS nel periodo in cui è stato sferrato l'attacco.

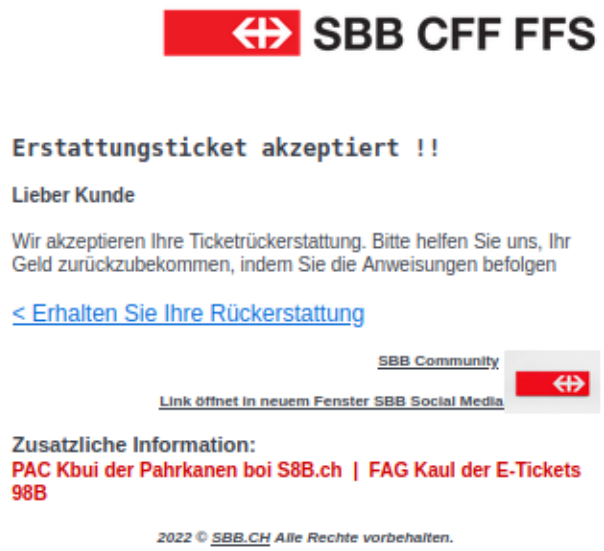

Fig. 6: Tentativo di phishing riguardante un rimborso fasullo di un biglietto delle FFS.

4.3.2 Tentativi di phishing sempre più professionali riguardanti Microsoft Office 365: collaboratori nel mirino

I dati di accesso a Microsoft Office 365 sono particolarmente interessanti agli occhi degli aggressori perché questi account possono essere sfruttati come punto di partenza per ulteriori attacchi, come la truffa mediante la manipolazione di una fattura. Questo tipo di frode può produrre danni potenziali ingenti, come si desume dalle 45 segnalazioni ricevute e dal danno pari a quasi mezzo milione di franchi notificato all'NCSC nel periodo di riferimento. Anche qui si ipotizza un numero elevato di attacchi non segnalati. I truffatori esaminano gli account violati e individuano le fatture emesse per poi modificarvi il numero IBAN a loro favore. In seguito la fattura viene nuovamente inviata al contraente con un pretesto, invitandolo a utilizzare il nuovo IBAN. Con l'accesso all'account aziendale di Microsoft Office 365, gli aggressori ottengono anche i dati interni all'azienda, utili per attacchi d'ingegneria sociale nei confronti di altri collaboratori o sfruttabili per un ricatto. Spesso gli hacker creano anche una regola di inoltro che consente loro di ricevere tutte le e-mail in arrivo della vittima. In tal modo, quando quest'ultima si rende conto di essere stata truffata e i dati di accesso vengono modificati, i truffatori continuano a ricevere tutte le e-mail. Non sorprende quindi che i phisher facciano di tutto per impossessarsi dei dati di accesso dei collaboratori. I tentativi sono sempre più professionali e, di conseguenza, più difficili da individuare. I collaboratori devono quindi essere formati regolarmente e si consiglia di utilizzare l'autenticazione a due fattori laddove possibile. Questa garantisce un ulteriore livello di protezione per evitare che gli account di Microsoft Office 365 vengano violati.

Fig. 7: Presunta proposta di progetto scaricabile da un server. Sullo sfondo si intravede un documento. Per poterlo aprire è richiesta la password dell'account di Microsoft Office 365.

4.4 Segnalazioni di malware e hacking

4.4.1 Numero di ransomware invariato

Nel secondo semestre del 2022 sono state registrate 155 segnalazioni di malware. La tendenza è in forte calo rispetto al periodo precedente. Nel primo semestre del 2022 questo numero era superiore di quasi quattro volte (592 segnalazioni). La diminuzione è riconducibile all'assenza di grande ondate di attacchi. Un anno fa, 405 segnalazioni erano dovute al solo malware «FluBot». Nell'anno in rassegna non è stato riportato alcun caso di questo tipo.

Il numero di ransomware è rimasto tuttavia invariato. Le 76 segnalazioni pervenute rappresentano quasi la metà di tutti i tentativi di attacco della categoria riguardante i malware. Circa un terzo delle segnalazioni proviene da privati e due terzi da imprese. Queste ultime sono prese di mira in modo particolare dal ransomware Lockbit, noto per la crittografia dei dati ma anche per il furto degli stessi, nonché per la loro pubblicazione online se non viene pagato il riscatto. Si tratta di una doppia estorsione che sta diventando sempre più comune. Probabilmente tale tendenza si confermerà anche nel 2023. Molte aziende hanno capito la minaccia dei ransomware e hanno reagito di conseguenza adeguando la strategia di backup. Pertanto la semplice crittografia non è più redditizia per gli aggressori: la minaccia di pubblicare i dati accresce la possibilità di ottenere il riscatto. Altre famiglie di ransomware segnalate che hanno preso di mira le aziende nell'ultimo semestre sono «Play», «Medusalocker», «Blackcat», «Magniber»

e «Makop». Nella maggior parte dei casi, il vettore di entrata non si conosceva ancora al momento della segnalazione. Spesso però la prima infezione è dovuta a una vulnerabilità o a una configurazione errata. È quello che emerge anche da uno studio di Microsoft, secondo cui l'80 per cento degli attacchi di ransomware è riconducibile a errori generali di configurazione di software e dispositivi.[4] Il rischio di un attacco di ransomware può essere ridotto in maniera efficace grazie a una gestione tempestiva delle patch, a regolari controlli della configurazione del sistema nonché all'utilizzo costante dell'autenticazione a due fattori per i servizi di accesso.

Nel caso di attacchi a privati, i dispositivi di archiviazione di rete (NAS) continuano a essere l'obiettivo principale degli aggressori. Il malware «Deadbolt» è quello più ricorrente, come riscontrato nelle sette segnalazioni pervenute. I dispositivi direttamente accessibili da Internet sono particolarmente esposti alle minacce. Vengono scansionati in modo sistematico al fine di ricercare vulnerabilità o configurazioni errate, ad esempio una password debole. Perciò è fondamentale mantenere i sistemi sempre aggiornati e proteggere l'accesso in modo adeguato.

«Qakbot» è ancora la famiglia di malware più attiva. Nel secondo semestre del 2022 l'NCSC ha ricevuto 20 segnalazioni. Tale malware si diffonde via e-mail. Una caratteristica di «Qakbot» consiste nell'utilizzare e collegare scambi di e-mail reali, sottratti in occasione di precedenti attacchi. In questo modo i cibercriminali cercano di conquistare la fiducia del destinatario, in quanto conosce la comunicazione e i presunti mittenti. L'obiettivo è spingere la vittima ad aprire il link.

4.4.2 Segnalazioni di hacking ancora in forte ascesa

Le segnalazioni che rientrano nella categoria di hacking sono aumentate sensibilmente. Rispetto al semestre precedente il numero è quasi raddoppiato (276 segnalazioni). Gli account dei social media (108 segnalazioni) rappresentano il bersaglio preferito. Nel frattempo i truffatori sfruttano gli account dei social media violati nell'ambito della «fake sextortion» per avvalorare i loro tentativi di falsa estorsione (cfr. sotto). Un altro frequente utilizzo degli account hackerati consiste nell'inserimento di annunci pubblicitari di truffe dell'investimento. Soprattutto nel caso di account con molti follower, questa è una trappola molto diffusa per trasmettere informazioni su offerte dubbie al maggior numero possibile di potenziali vittime.

4.4.3 Casi di falsa estorsione con attacchi reali

Finora le cosiddette e-mail di «fake sextortion» erano meri bluff. I malintenzionati inviano un'e-mail in cui affermano di aver raccolto foto o video che ritraggono il destinatario dell'e-mail durante una presunta visita su siti pornografici. I ricattatori minacciano di pubblicare tali foto o video se non viene pagato un riscatto entro una certa data. Nell'anno in rassegna l'NCSC ha ricevuto 1138 segnalazioni riguardanti e-mail di questo tipo. Di solito i cibercriminali mentono: non hanno alcun accesso al computer della vittima e sperano che questa si lasci intimidire e paghi il riscatto. Lo scorso semestre sono stati però segnalati anche casi in cui gli account di posta elettronica e vari account di social media venivano violati poco prima o subito dopo l'e-mail ricattatoria. In 33 casi i truffatori hanno caricato materiale pornografico che ha comportato il blocco immediato degli account dei social media, seguito da una relativa notifica. Gli aggressori tentano così di spaventare la vittima e di indurla a effettuare il pagamento. I dati di accesso

[4] Cyber Signals (microsoft.com)

possono provenire o da vecchie fughe di dati o da vecchi tentativi di phishing. Tuttavia, rispetto al numero complessivo di e-mail di «fake sextortion» segnalate, il numero di casi con la variante che prevede anche la violazione degli account è ancora molto bassa. Ciò denota che le combinazioni di password e login utilizzate non sono attuali e non funzionano quindi per tutte le potenziali vittime. Probabilmente si tratta di un uso secondario di password e login, acquistabili a basso costo nel dark web.

4.5 Diverse segnalazioni

4.5.1 L'impotenza di fronte allo «spoofing» telefonico

Anche le segnalazioni riguardanti casi di «spoofing» telefonico hanno registrato un aumento senza precedenti. Gli aggressori manipolano il numero di telefono visualizzato in modo tale da far apparire un numero diverso con l'intento di non destare sospetto nella vittima. Mentre nel 2021 sono pervenute soltanto 26 segnalazioni, nel secondo semestre del 2022 l'NCSC ne ha già ricevute 781. Il motivo risiede in un nuovo approccio da parte di call center esteri di dubbia affidabilità. Per fare in modo che le vittime ricevano il maggior numero possibile di chiamate pubblicitarie, gli aggressori utilizzano numeri di telefono svizzeri. Questo approccio, che a prima vista sembra innocuo, può avere conseguenze importanti per la persona a cui appartiene il numero falsificato. Se la chiamata rimane senza risposta e il numero viene visualizzato sul display, molti richiamano inondando di chiamate il proprietario. Poiché i call center utilizzano lo stesso numero per settimane o persino mesi, ciò può risultare snervante per le vittime.

Purtroppo non si può fare molto per evitare queste chiamate dei call center. Siccome provengono dall'estero, l'obbligo di verifica riguardante l'utilizzo dei numeri, che gli operatori telefonici svizzeri sono tenuti ad adempiere, non è applicabile. Tale obbligo si applica soltanto se la chiamata proviene dalla loro rete. Se le chiamate non cessano, l'unica soluzione è cambiare numero di telefono.

5 Situazione

5.1 Accesso iniziale

I cibercriminali sono organizzati in base all'attività svolta e si specializzano nelle singole fasi riguardanti un ciberattacco. Ottenere l'accesso ai sistemi informatici da remoto o agli account degli utenti è la prima tappa nella maggior parte dei ciberattacchi. L'accesso iniziale può avvenire in vari modi e, una volta ottenuto, può essere trasmesso ad altri aggressori.

5.1.1 Nome utente / password

I truffatori si impossessano delle credenziali per l'accesso perlopiù tramite attacchi di phishing (cfr. n. 4.3). Ciò significa che gli utenti stessi trasmettono inconsapevolmente le credenziali agli aggressori. Inoltre, i dati di accesso possono essere intercettati mediante malware («keylogger») quando vengono inseriti in un dispositivo infetto.

Le credenziali per l'accesso da remoto tramite «Remote Desktop Protocol» (RDP) o «Virtual Private Network» (VPN) sono spesso utilizzate in modo illecito per penetrare nelle rete informatiche aziendali.

Raccomandazioni

Utilizzando un'autentificazione a due o più fattori è possibile proteggersi da questa minaccia. La combinazione di nome utente e password non è sufficiente per accedere al sistema protetto o all'account utente, bensì sono necessarie altre informazioni come il codice usa e getta inviato per SMS o l'autenticazione tramite applicazione.

5.1.2 Malware (trojan)

I software dannosi che aprono un varco nel sistema dopo la loro installazione costituiscono un metodo diventato ormai consueto per ottenere l'accesso iniziale.

Il vettore più utilizzato per diffondere trojan continua a essere la posta elettronica. Spesso le e-mail riguardano argomenti quotidiani come offerte, consegne o fatture. Talvolta si fa leva su informazioni esclusive concernenti temi di attualità come la guerra in Ucraina, catastrofi naturali o eventi sportivi per stuzzicare la curiosità degli utenti. In molti casi, poi, per indurre il destinatario dell'e-mail a compiere determinate azioni senza riflettere troppo, si fa credere che sia necessario agire in fretta. Da un lato, tali e-mail vengono inviate in massa a un gran numero di destinatari (malspam). Dall'altro, vengono sfruttati vecchi scambi di e-mail ottenuti in precedenza da account compromessi o da server di posta elettronica violati e vengono contattati i partecipanti alle conversazioni («thread hijacking») e installati trojan nei loro dispositivi.

Un'altra variante che intende indurre gli utenti a installare un malware consiste nell'acquisto di spazi pubblicitari online o nell'inserimento dei risultati sponsorizzati nei motori di ricerca (malvertising). In questo caso si fa credere che il software desiderato (ad es. un browser, un'app di comunicazione o un lettore video) sia disponibile nell'inserzione corrispondente. Insieme al software desiderato (gratuito), però, viene installato un trojan. Un metodo analogo consiste nell'attirare gli utenti tramite link pubblicitari su una pagina in cui si spiega che la versione del browser non è più attuale e che è necessario un aggiornamento. Poiché il sito web riconosce il browser di accesso, la pagina viene adattata in base al motore di ricerca in uso. Cliccando sul pulsante dell'aggiornamento viene scaricato un file che, una volta eseguito, installa il trojan. Questi aggiornamenti fasulli possono essere diffusi anche tramite siti web violati.

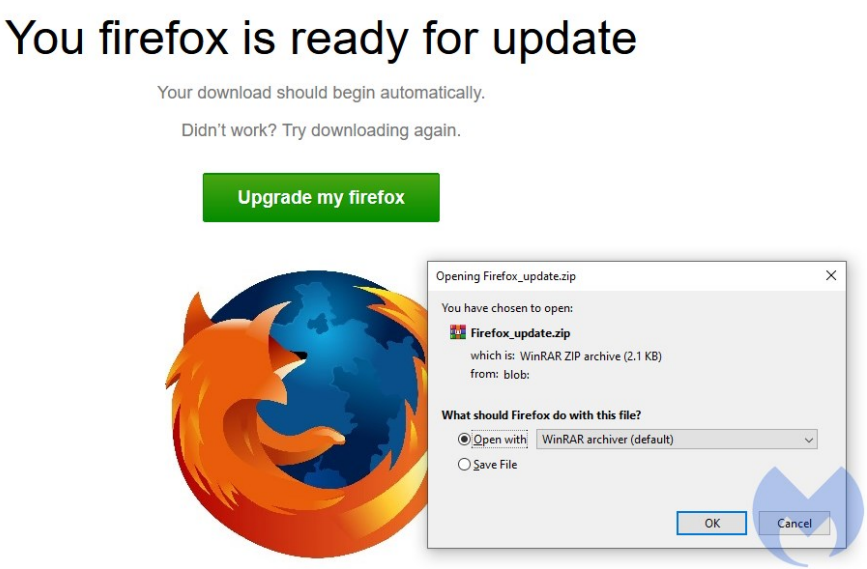

Fig. 8: Aggiornamento fasullo (fonte: Malwarebytes.com).

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, verificate di essere sul sito web del produttore o su un altro sito affidabile (ad es. in una rivista di informatica). Siate prudenti quando si apre 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.

5.1.3 Sfruttamento delle vulnerabilità

Non appena viene individuata una vulnerabilità in un prodotto, vari attori iniziano a cercare su Internet i sistemi esposti. Dopo qualche ora o giorno la falla inizia a essere sfruttata. Tuttavia, anche le vulnerabilità note da tempo e per le quali sarebbe disponibile una patch vengono sfruttate regolarmente. Il catalogo realizzato dall'autorità di cibersicurezza statunitense CISA riguardante le vulnerabilità attualmente sfruttate[5] viene costantemente aggiornato con l'inserimento delle vecchie vulnerabilità che potrebbero essere già risolte dagli utenti tramite una gestione efficace degli aggiornamenti.[6]

Oltre a errori di programmazione da parte degli sviluppatori, risolvibili tramite una patch, anche le configurazioni scelte per l'implementazione di prodotti possono comportare vulnerabilità. Diversi produttori forniscono istruzioni in merito alla configurazione per rafforzare i loro prodotti.

Raccomandazioni

Quando utilizzate nuovi prodotti verificate la relativa configurazione per gli aspetti concernenti la sicurezza e la protezione dei dati. Assicuratevi che siano attivate soltanto le funzionalità di cui avete bisogno.

Privati e aziende dovrebbero quindi mantenere sempre aggiornati i software su tutti i loro dispositivi, possibilmente attraverso la funzione di aggiornamento automatico.

I software che hanno raggiunto la fine del loro ciclo di vita e non presentano più aggiornamenti da parte del produttore vanno sostituiti.

L'NCSC informa regolarmente le organizzazioni esposte ad attacchi a causa di sistemi obsoleti.[7] Questi suggerimenti sono forniti da specialisti nel settore della cibersicurezza che setacciano Internet alla ricerca dei sistemi a rischio. Allo stesso modo anche i criminali possono

---

5 Known Exploited Vulnerabilities Catalog (cisa.gov)

6 Adobe, Apple, Cisco, Microsoft Flaws Make Up Half of KEV Catalog (darkreading.com)

7 È giunta l'ora di correggere le vulnerabilità di Microsoft Exchange Server (ncsc.admin.ch);
Microsoft Exchange presenta ancora lacune (ncsc.admin.ch);
Ancora oltre 2800 server Microsoft Exchange vulnerabili in Svizzera («ProxyNotShell») (ncsc.admin.ch);
Server Microsoft Exchange ancora vulnerabili in Svizzera («ProxyNotShell») nonostante gli avvisi dell'NCSC (ncsc.admin.ch)

individuare e attaccare i sistemi vulnerabili. I gestori dei sistemi non dovrebbero quindi aspettare di ricevere un avviso da parte dell'NCSC. Si consiglia vivamente di procurarsi un proprio sistema efficace di gestione dei software, con un inventario e procedure per gli aggiornamenti.[8] Occorre intervenire al più tardi quando l'organizzazione riceve una lettera raccomandata dall'NCSC.

5.2 Software dannosi (malware)

5.2.1 Diffusione di malware

Il grafico sottostante mostra le famiglie di malware che l'NCSC ha analizzato e identificato lo scorso semestre. Individuati grazie a diverse fonti (sensori, segnalazioni da parte di responsabili della sicurezza di infrastrutture critiche, cittadini e PMI), i file e i codici vengono analizzati e attribuiti a una famiglia di malware. In seguito, l'NCSC trasmette gli indicatori di compromissione («indicator of compromise», IoC) riscontrati ai gestori delle infrastrutture critiche, in modo che questi possano proteggersi.

Analisi dell'NCSC concernente le famiglie di malware

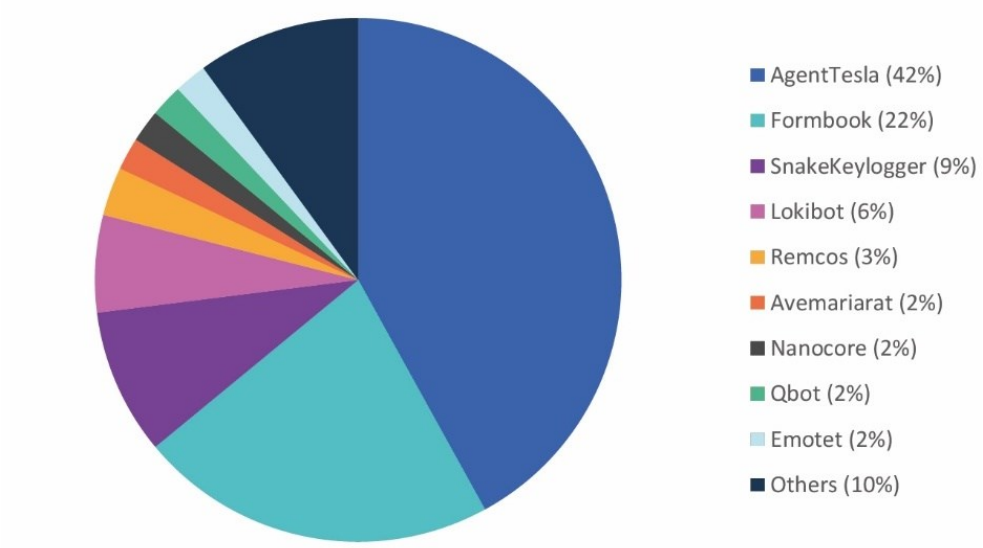

Fig. 9: Analisi dell'NCSC concernente le famiglie di malware diffuse in Svizzera nel secondo semestre del 2022.

5.2.2 Ransomware

Gli attacchi di ransomware continuano a rappresentare una minaccia frequente, probabilmente la più grave per le organizzazioni in Svizzera. Nel secondo semestre sono state prese di mira soprattutto le piccole e medie imprese attive nel settore industriale nonché i fornitori di servizi informatici. Gli sviluppatori di ransomware perseguono nuove strategie e metodi per infiltrarsi nei sistemi e ricattare le vittime. A titolo di esempio citiamo la nuova versione di un ransomware, un codice nel linguaggio di programmazione Rust per Windows e Linux e la pubblicazione dei dati su siti web regolari (non soltanto nel dark web). Per massimizzare i profitti

[8] Cfr. Rapporto semestrale 2021/1 (ncsc.admin.ch), n. 3.2

spesso i cibercriminali ricorrono a un doppio ricatto: i dati vengono esfiltrati dalla rete compromessa prima che questi vengano crittografati. Così possono ricattare la vittima minacciandola di pubblicare i dati. Visto il crescente numero di casi di ransomware, della disponibilità dei malware come servizio («ransomware as a service», RaaS) e del numero sempre più elevato di ceppi e famiglie di ransomware, le aziende attive nel settore della cibersicurezza collaborano strettamente con gli organi statali al fine di trovare le chiavi di decifrazione e sviluppare programmi di decodifica.

5.2.2.1 Ciberincidenti in Svizzera: alcuni esempi

Play: quando un incidente riguarda terzi

In seguito a un attacco ransomware probabilmente lanciato dal gruppo Play, a fine novembre un fornitore di servizi di computing basato sul cloud attivo nel Cantone di Berna ha dovuto chiudere i suoi centri di calcolo. I backup effettuati quattro giorni prima hanno permesso di salvare parte dei dati. L'incidente ha avuto conseguenze per tutti i clienti del fornitore: alcuni non hanno più potuto accedere al servizio di cloud, emettere fatture o calcolare e pagare gli stipendi. Tuttavia, durante l'attacco i dati non sono stati esfiltrati. Nel corso dell'anno sono stati segnalati episodi analoghi a nome di Play anche in altri Cantoni.

Doppia estorsione: attacco con crittografia e perdita di dati

Il 5 settembre 2022 una fabbrica di cioccolato è stata vittima di un attacco ransomware che ha colpito duramente la produzione, la logistica e la gestione aziendale. Due settimane dopo l'attacco le unità colpite hanno ripreso l'attività. Tuttavia, l'impresa ha confermato che il ciberattacco aveva probabilmente provocato una fuga di dati. Un mese dopo, il gruppo ransomware BianLian ha pubblicato nel dark web file relativi all'attività dell'impresa.

Il gruppo suddetto utilizza un malware sviluppato ad hoc scritto nel linguaggio di programmazione Go.[9] BianLian ha iniziato la sua attività online nel dicembre del 2021 e ha intensificato i suoi attacchi nel luglio del 2022. Ha poi ampliato in modo massiccio la sua infrastruttura di comando e di controllo (C2) nell'agosto del 2022.

5.2.2.2 Ciberincidenti all'estero: attacchi nel settore dell'energia

Nel rapporto semestrale 2022/1 l'NCSC ha presentato alcuni esempi di rami economici colpiti da attacchi ransomware, sottolineando il fatto che i criminali sembrano concentrare la loro attenzione su governi, autorità e infrastrutture energetiche. Questa tendenza è stata confermata nel secondo semestre, in particolare per quanto riguarda il settore dell'energia. L'aumentato interesse dei truffatori può anche essere dovuto al fatto che il settore dell'energia è associato alle infrastrutture critiche che, come tali, devono essere sempre operative e, nell'attuale contesto geopolitico, sono sottoposte a pressioni particolari. Diversi fornitori di energia europei hanno accusato attacchi ransomware.[10] Gli aggressori che hanno rivendicato la responsabilità di questi attacchi, come nel caso di BlackCat ed Everest, sono gruppi filorussi e ciò non sor-

---

9 MalwareHunterTeam on Twitter: A BianLian x64 ransomware sample (twitter.com)

10 Nel 2022, in Italia sono stati colpiti da attacchi ransomware importanti gestori di servizi energetici quali GSE SpA e Amalfitana Gas Srl nonché la società petrolifera Eni, in Lussemburgo il fornitore di rete elettriche e gas naturale Creos Luxembourg SA e in Grecia il maggiore distributore di gas naturale DESFA.

prende. Finora i fornitori di energia in Svizzera sono stati risparmiati da tali attacchi. Al momento si ritiene piuttosto improbabile che il nostro Paese venga preso di mira dagli aggressori. Tuttavia, non si possono escludere attacchi opportunistici contro sistemi vulnerabili o danni collaterali derivanti da attacchi perpetrati contro fornitori europei.

5.2.2.3 Panoramica degli attori più attivi e dei vettori d'infezione più ricorrenti

Nel 2022 il ransomware più utilizzato in Svizzera è stato Lockbit (nelle versioni 2.0 e 3.0 Black), seguito da Deadbolt e Play (cfr. n. 4.4.1). Su scala mondiale, il gruppo Lockbit è rimasto quello dominante, seguito da BlackBasta e BlackCat. Nel giro di alcuni mesi altri gruppi si sono inaspettatamente posizionati in cima alla classifica, senza però rimanervi a lungo. Ne sono un esempio Hive, Sparta, Cuba, Royal e BianLian.

Lockbit Black si riconferma al primo posto con l'aggiornamento della versione

Nel luglio del 2022 il gruppo Lockbit ha annunciato lo sviluppo della versione 3.0 del suo ransomware. L'aggiornamento ha avuto conseguenze in Svizzera a partire dal novembre 2022: la polizia ha registrato un aumento dei casi correlati a tale malware.

Tuttavia, alcuni settori sono stati risparmiati, in quanto il codice deontologico di Lockbit (o meglio i termini e le condizioni generali del gruppo «ransomware as a service») vieta la crittografia dei dati di scuole e ospedali. Ciononostante, un ospedale pediatrico canadese è stato vittima di un simile attacco. È emerso che gli autori erano partner (cosiddetti «affiliati») del gruppo Lockbit, il quale si è scusato sui social media annunciando l'estromissione degli affiliati. Lockbit ha inoltre fornito all'ospedale un decrittatore gratuito per decriptare i dati.

Nell'ambito di un'indagine su Lockbit le autorità francesi e canadesi, in collaborazione con l'FBI, sono riuscite a identificare circa 1800 vittime effettive o presunte.[11] I sistemi infetti presentavano una falla di sicurezza nei loro firewall FortiGate o SonicWall. Le organizzazioni interessate in Svizzera sono state informate dalla polizia.

Agenda e Hive: Rust rinnova i vecchi ransomware

Molti responsabili di attacchi ransomware hanno sviluppato una versione rielaborata del loro software nel linguaggio multipiattaforma Rust, che consente di utilizzare il malware su Windows e su Linux. Ne è un esempio Agenda (noto anche come Qilin), originariamente scritto nel linguaggio di programmazione Go. Attualmente gli autori di Agenda sembrano essere impegnati a migrare il codice del loro ransomware su Rust, poiché nelle ultime edizioni dei software mancano alcune funzioni che erano incluse nel codice originale. Agenda e il ransomware Royal funzionano con una crittografia parziale (denominata anche «crittografia intermittente»). In questo caso, la percentuale del contenuto del file da crittografare è determinata da parametri prestabiliti. Le crittografie possono essere così eseguite più in fretta, evitando i rilevamenti basati principalmente sulle funzioni di lettura e scrittura dei file. Gli aggressori utilizzano sempre più spesso il linguaggio di programmazione Rust perché è più difficile da analizzare e molti programmi antivirus non riescono a intercettare bene i malware scritti con questo linguaggio. In Svizzera un'amministrazione comunale nel Cantone di Zurigo è stata criptata dal ransomware Agenda. Il ripristino dei dati è stato possibile grazie ai backup.

---

[11] Police arrest suspected LockBit operator as the ransomware gang spills new data (techcrunch.com)

BlackCat e IceFire: pubblicazione di dati rubati su Internet

Una nuova tecnica di estorsione del gruppo ransomware ALPHV/BlackCat consiste nel creare una copia del sito web della vittima, sul quale l'aggressore pubblica i dati rubati con l'intento di esercitare maggiore pressione sulla vittima. Sul sito web copiato, BlackCat sostituisce le rubriche e le sottopagine originali per selezionare i dati rubati. La pagina replicata viene poi pubblicata su Internet in modo tale che i file rubati siano disponibili più facilmente sul dark web. Il sito web oggetto del ricatto viene spesso creato su un dominio che presenta errori di battitura.[12] Tale strategia è più problematica rispetto al semplice rilascio di dati tramite un sito web sulla rete Tor nel dark web, poiché i dati forniti su una normale pagina Internet sono facilmente consultabili da chiunque. Siccome la vittima non vuole che i clienti o altre persone vedano i dati, questo metodo mette sotto pressione la vittima inducendola a pagare il riscatto.

L'idea è stata ripresa dal gruppo ransomware IceFire, che a metà agosto del 2022 ha attaccato un'impresa svizzera. IceFire ha fatto la sua prima apparizione nel marzo del 2022 e, al fine di esercitare maggiore pressione sulle sue vittime, ha adottato la stessa tecnica di BlackCat.

Play (noto anche come PlayCrypt): nel mirino vittime vicine al governo

Già dal suo debutto nell'estate del 2022 il gruppo Play ha focalizzato la sua attenzione sui servizi statali. Si tratta di una rarità, considerato il carattere repressivo del procedimento penale applicato a simili attacchi. Play sferra attacchi soprattutto in America Latina. Tuttavia, il gruppo si è fatto conoscere anche in altri continenti e in settori diversi da quello amministrativo.

Play è noto per la sua strategia di «big game hunting», ossia colpisce organizzazioni finanziariamente forti. Utilizza ad esempio «Cobalt Strike» per la fase post-attacco e «SystemBC RAT» per ottenere persistenza. Di recente gli hacker di Play hanno iniziato a sfruttare le vulnerabilità «ProxyNotShell» su Microsoft Exchange. Dalle analisi emergono parallelismi tra le varianti di ransomware «Play», «Hive» e «Nokoyawa».

BianLian e MegaCortex: decodifica di dati tramite decrittatori...

Solo sei mesi dopo il picco registrato nell'estate del 2022, nel gennaio del 2023 è stato rilasciato un decrittatore gratuito (programma per la decodifica di file criptati da ransomware) per il ceppo BianLian.[13] In un'operazione congiunta tra Europol e la polizia cantonale di Zurigo è stato arrestato anche lo sviluppatore del ransomware MegaCortex, per cui è stato possibile creare un software di decodifica per questo ceppo. Su Internet sono ora disponibili numerosi programmi di decodifica gratuiti.[14] Le imprese attive nel settore della cibersicurezza si adoperano per sviluppare in tempi brevi tali programmi al fine di contrastare la diffusione incontrollata di ceppi di ransomware.

... e tramite chiavi di cifratura (Deadbolt)

Nell'ottobre del 2022 la polizia dei Paesi Bassi è riuscita a ottenere 150 chiavi di cifratura del gruppo ransomware Deadbolt grazie a uno stratagemma realizzato nell'ambito dei pagamenti in bitcoin.[15] Anche in Svizzera diversi dispositivi sono stati presi di mira da Deadbolt, che cripta

---

12 Il «typosquatting» è un attacco di ingegneria sociale che consiste nell'utilizzare domini che presentano refusi («typo»), ad es. «adimn.ch», «adnim.ch» o «adrnin.ch» anziché «admin.ch».

13 Decrypted: BianLian Ransomware (avast.io)

14 Cfr. ad es. The No More Ransom Project (nomoreransom.org)

15 Police tricked a ransomware gang into handing over its decryption keys. Here's how they did it (zdnet.com)

principalmente i dispositivi NAS prodotti dall'azienda QNAP. L'ottenimento di queste chiavi è stato utilissimo perché ha permesso a diverse vittime di decriptare i propri supporti di dati. Ora è possibile verificare online se è disponibile una chiave per un dispositivo infettato da Deadbolt.[16]

Conclusioni, previsioni e raccomandazioni

Nel caso di attacchi ransomware accade sempre più spesso che i dati (in parte sensibili) vengano criptati e sottratti come tentativo di doppia estorsione. Alcuni aggressori non si preoccupano neppure di criptare i sistemi, bensì si limitano a minacciare di pubblicare i dati della vittima.

I ransomware possono provocare notevoli danni, in particolare quando colpiscono anche i sistemi di protezione dei dati (backup). Sul sito web dell'NCSC sono descritti aspetti importanti relativi alla gestione di ciberincidenti: Sono vittima di un attacco ransomware. E adesso? (ncsc.admin.ch) e C'è stata una fuga di dati. E adesso? (ncsc.admin.ch).

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

Come recentemente dimostrato nel contesto della guerra in Ucraina, nei conflitti geopolitici talvolta possono verificarsi anche sabotaggi informatici distruttivi.[17] Per produrre un impatto sui processi fisici, è quasi inevitabile manipolare la tecnologia operativa e i suoi sistemi di controllo. Molto di rado si agisce direttamente sui processi fisici controllati; nella stragrande maggioranza dei casi si attacca l'infrastruttura server e di rete con l'obiettivo di interrompere l'esercizio.[18]

5.3.1 Tentativi di sabotaggio nel quadro di conflitti

All'inizio della guerra in Ucraina[19] sono stati respinti tentativi mirati di sabotaggio mediante software dannosi specifici per i sistemi di approvvigionamento di energia elettrica[20], è stata esposta l'infrastruttura di attacco[21] da parte dei medesimi attori ed è stata pubblicata un'intera serie di strumenti di attacco[22] prima del loro impiego. Nel secondo semestre del 2022 i tentativi di sabotaggio si sono limitati all'utilizzo di programmi wiper distruttivi [23] e agli attacchi camuffati da ransomware[24]. Non sono più state osservate capacità specifiche volte a manipolare sistemi industriali. Gli attacchi sono stati però diretti contro i sistemi informatici di organizzazioni di trasporto in[25] Ucraina e Polonia.

---

16 Deadbolt Decryption (responders.nu)

17 Si veda in particolare «Stuxnet» nel rapporto semestrale 2010/2 (ncsc.admin.ch), n 4.1 e 5.1) e Triton/Trisis nel rapporto semestrale 2017/2 (ncsc.admin.ch), n 5.3.2.

18 How Many ICS-OT Directed Attacks In 2022? (linkedin.com)

19 Rapporto semestrale dell'NCSC 2022/1, n. 3 e n. 5.4

20 Industroyer2: Industroyer reloaded (welivesecurity.com)

21 New Sandworm malware Cyclops Blink replaces VPNFilter (ncsc.gov.uk)

22 APT Cyber Tools Targeting ICS/SCADA Devices (cisa.gov)

23 Russian APT groups continue their attacks against Ukraine with wipers and ransomware (eset.com)

24 RansomBoggs: New ransomware targeting Ukraine (welivesecurity.com)

25 New "Prestige" ransomware impacts organizations in Ukraine and Poland (microsoft.com)

Gruppi di hacktivisti come OneFist[26] e Ghostsec[27] hanno affermato di aver causato guasti a impianti industriali. Tuttavia, non è stato possibile né confermare queste dichiarazioni né verificarle in modo indipendente. Gli estratti presentati dai gruppi indicano semplici tentativi di manipolazione di interfacce utente di sistemi di controllo industriali accessibili da Internet e scarsamente protetti.

5.3.2 In primo piano: situazione critica nell'approvvigionamento energetico

La guerra in Ucraina ha provocato, come effetto collaterale, la compromissione della sicurezza nell'approvvigionamento energetico in Europa e quindi anche in Svizzera, dove ne ha risentito specialmente l'approvvigionamento di gas ed elettricità. Per ridurre la probabilità che si verifichi una carenza di energia, è stata lanciata una campagna di risparmio energetico.[28]

In una simile situazione critica, se andasse a segno un ciberattacco contro i sistemi di controllo delle catene di approvvigionamento le conseguenze sarebbero ben più gravi rispetto a quelle che si produrrebbero se fossero disponibili sufficienti possibilità compensatorie. Se il conflitto non si allargherà ad altri territori europei, un tentativo di sabotaggio statale mirato[29] contro i sistemi di approvvigionamento svizzeri rimane improbabile. Il pericolo maggiore è rappresentato dagli attacchi ransomware.[30] Se le crittografie che ne derivano paralizzano i sistemi coinvolti nell'approvvigionamento energetico, ciò può comportare limitazioni e interruzioni dell'esercizio.[31]

Anche la sicurezza fisica dei sistemi svolge un ruolo importante in questo contesto. L'esempio della separazione meccanica dei cavi di controllo della Deutsche Bahn[32] mostra da un lato il pericolo reale di attacchi di sabotaggio in loco[33] e dall'altro sottolinea l'importanza di predisporre misure per ripristinare la prontezza operativa al fine di rafforzare la resilienza dell'intero sistema.

Conclusione / raccomandazioni

Le considerazioni sulla resilienza dei sistemi e delle organizzazioni sono essenziali per preservare l'esercizio degli impianti industriali anche in situazioni critiche. Ciò include anche la formazione e la formazione continua del personale.

Misure appropriate sono contenute negli standard minimi per le TIC pubblicati dall'UFAE o nei relativi standard settoriali: Standard minimi per le TIC (ncsc.admin.ch).

Sul proprio sito, l'NCSC raccomanda una serie di misure di protezione dei sistemi di controllo industriali (ICS) (ncsc.admin.ch).

---

26 The Increasing Threat Posed by Hacktivist Attacks (forescout.com)
27 Country-Specific ICS Targeting: Shining a Light on GhostSec (otorio.com)
28 Energia: il Consiglio federale lancia una campagna di risparmio energetico (admin.ch)
29 «La sicurezza della Svizzera 2022»: il Servizio delle attività informative della Confederazione presenta il suo nuovo rapporto sulla situazione (admin.ch)
30 Dragos Industrial Ransomware Analysis: Q4 2022 (dragos.com)
31 Cybersecurity Research Report January 2023 (nozominetworks.com)
32 Sabotage bei der Bahn: Viele vertrauliche Infos sind offen zugänglich (heise.de)
33 BfV-Sicherheitshinweis für die Wirtschaft 04/2022 (wirtschaftsschutz.info)

5.4 Vulnerabilità

5.4.1 Sistemi con file di configurazione accessibili al pubblico

L'NCSC riceve regolarmente segnalazioni di vulnerabilità da parte di ricercatori in materia di cibersicurezza tramite il processo «Coordinated Vulnerability Disclosure»[34]. Nel semestre in rassegna sono state segnalate diverse vulnerabilità riconducibili a un'errata configurazione del software: i relativi file si trovano in una directory su un server web e sono accessibili senza restrizioni.

Un esempio comune sono i file realizzati dal software nel versionamento Git. Questo software genera una directory denominata «.git», in cui viene memorizzato l'intero codice sorgente. Se la cartella è accessibile e consultabile tramite un server web, un aggressore con conoscenze tecniche può ottenere dati potenzialmente sensibili come dati di accesso o password.

L'NCSC è riuscito a identificare 1300 sistemi colpiti in Svizzera e ha informato gli operatori interessati.

Git non è l'unico software a generare file di configurazione e cartelle nascoste; le pagine profilo PHP, un componente del framework Symfony, sono un altro esempio.[35] Anche i file di testo come «.env» sono spesso impiegati per memorizzare le chiavi di accesso e le password che un sistema utilizza. Se questi non dispongono dei diritti di accesso corretti, anch'essi possono essere letti e usati in modo illecito da un malintenzionato.

L'NCSC collabora attivamente con i ricercatori in materia di cibersicurezza al fine di informare gli operatori colpiti e sensibilizzarli in merito a rischi e pericoli che gli errori di configurazione possono comportare.[36]

Conclusione / raccomandazioni

I file di configurazione come la cartella «.git» non dovrebbero mai essere liberamente accessibili su Internet. Se la cartella non può essere eliminata in tempi brevi, l'accesso dovrebbe essere perlomeno limitato e protetto in modo adeguato (ad es. tramite regole «.htaccess» o restrizioni tecniche simili, a seconda della tecnologia utilizzata).

Misure preventive come la verifica e l'adeguamento del processo di sviluppo sono ancora più efficaci. Ciò dovrebbe garantire che vengano memorizzati soltanto i dati desiderati e previsti a tale scopo («build file»). I dati sensibili o segreti (password, chiavi API ecc.) non dovrebbero mai essere memorizzati nel codice sorgente o nell'applicazione stessa («hardcoded»). Bisognerebbe almeno evitare che vengano memorizzati nella directory «.git», bensì che vengano ignorati («gitignore file»). Queste misure di sicurezza fondamentali e le buone prassi devono essere sempre rispettate.

34 Segnalazione di una falla di sicurezza (Coordinated Vulnerability Disclosure, CVD) (ncsc.admin.ch)
35 Covid-Center & andere Webseiten: Bedienen Sie sich! (dnip.ch)
36 Le directory.git non protette costituiscono un rischio per la sicurezza in Internet (ncsc.admin.ch)

5.4.2 ProxyNotShell

Alla fine di settembre 2022 un'impresa vietnamita attiva nel settore della cibersicurezza[37] ha riferito in merito ad attacchi avvenuti in tutto il mondo nell'agosto del 2022 contro infrastrutture critiche. Nell'analisi sono state riscontrate due vulnerabilità zero-day nei server di Microsoft Exchange che sono state sfruttate per il ciberattacco. La prima vulnerabilità (CVE-2022-41040) consiste in un attacco di tipo «server-side-request-forgery» (SSRF). Essa consente a un aggressore autenticato di lanciare la seconda vulnerabilità (CVE-2022-41082), ossia una «remote code execution» (RCE), la quale permette l'esecuzione di codici dannosi da remoto tramite Internet. Le due vulnerabilità sfruttate in contemporanea possono essere utilizzate per ottenere l'accesso a sistemi esposti.

Poco dopo Microsoft ha confermato le vulnerabilità riscontrate nei server Microsoft Exchange 2013, Microsoft Exchange 2016 e Microsoft Exchange 2019 e ha raccomandato di avviare misure urgenti. La vulnerabilità è stata denominata «ProxyNotShell» in quanto si riferisce a una vulnerabilità di Exchange apparsa nel 2021 chiamata «ProxyShell» (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207), che presentava alcune analogie con la nuova vulnerabilità.

Il 10 novembre 2022 Microsoft ha rilasciato gli aggiornamenti software che hanno permesso di eliminare le vulnerabilità. Il 18 novembre 2022 l'NCSC aveva individuato in Svizzera 2800 server vulnerabili in quanto non avevano lanciato gli ultimi aggiornamenti di sicurezza.[38] All'inizio di dicembre 2022 l'NCSC ha contattato i diretti interessati tramite lettera raccomandata.

Conclusione / raccomandazioni

La vulnerabilità «ProxyNotShell» è stata sfruttata in modo attivo prima che fosse disponibile una patch ufficiale. In questi casi è importante reagire rapidamente e seguire le raccomandazioni, che possono determinare anche la disattivazione del sistema finché è disponibile una patch ufficiale. Una strategia chiara per l'accesso diretto via Internet alle interfacce di gestione e alle applicazioni interne può ridurre la superficie esposta agli attacchi di un'organizzazione. Se vi sono applicazioni sensibili che devono essere accessibili via Internet, l'accesso deve essere dotato di una particolare protezione (tramite VPN con autenticazione a più fattori, un elenco degli IP autorizzati alla manutenzione ecc.). Se per una vulnerabilità sfruttata attivamente non esiste ancora una patch, una buona gestione degli accessi dall'esterno permette di guadagnare tempo per adottare le misure di difesa. Questo però non esonera dall'aggiornamento del sistema e dall'installazione delle patch non appena sono disponibili.

37 Two Microsoft Exchange zero-days exploited by attackers (helpnetsecurity.com)

38 Ancora oltre 2800 server Microsoft Exchange vulnerabili in Svizzera («ProxyNotShell») (ncsc.admin.ch)

5.4.3 Retbleed

Il 12 luglio 2022 il Politecnico federale di Zurigo (PFZ)[39] ha notificato una vulnerabilità nei microprocessori di Intel e AMD, denominata «Retbleed». Questa permette all'aggressore di accedere potenzialmente a qualsiasi area di memoria. Il termine «Retbleed», composto da «RET» e «bleed» («sanguinare» in inglese), si rifà a denominazioni esistenti di altre falle riscontrate, ad esempio «Heartbleed», che prevede anch'essa la lettura dei dati dalla memoria. «RET» è l'abbreviazione di «RETURN», un'istruzione di programma nei processori. È necessario prestare particolare attenzione alle infrastrutture condivise («shared infrastructure») e all'esecuzione di software non affidabili.

L'NCSC ha affiancato i ricercatori del PFZ nei lavori di coordinamento concernenti la pubblicazione e l'assegnazione dei numeri CVE. Per «Retbleed» sono stati assegnati i numeri CVE-2022-29900 (per i processori AMD) e CVE-2022-29901 (per i processori Intel).

Conclusione / raccomandazioni

«Retbleed» è una vulnerabilità molto complessa che finora non è stata sfruttata attivamente o perlomeno il suo sfruttamento non è noto.

La falla è tuttavia è soggetta a determinate condizioni per poter essere sfruttata, perciò il rischio per gli utenti è esiguo.

Intel e AMD stanno sviluppando delle patch al fine di ridurre al minimo ed eliminare la falla. È e rimane importante eseguire su un sistema soltanto software affidabili e diffidare di software sconosciuti. Inoltre, è fondamentale installare subito gli aggiornamenti e le patch dei produttori nonché seguire le relative raccomandazioni.

5.5 Fughe di dati

La sicurezza dei dati è una delle maggiori sfide della digitalizzazione per i proprietari dei dati, per i privati e le imprese, che trovano le loro informazioni nei record di dati. Nonostante l'accresciuta consapevolezza in merito alla sicurezza e alla protezione dei dati nello spazio digitale, per diversi motivi la loro fuga rimane un tema di attualità anche nel secondo semestre del 2022. Oltre alla scarsa protezione o manutenzione dei sistemi, la diffusione di dati sensibili è dovuta a errori umani e a ciberattacchi. Nei ciberattacchi, il furto di dati, spesso associato alla crittografia (cfr. n. 5.2.2), può essere utilizzato per ricattare la vittima e/o per vendere i dati al miglior offerente.

Sebbene, come riportato nei media, nella maggior parte dei casi si tratta di attacchi ransomware, va ribadito che una parte considerevole delle pubblicazioni contenenti dati sensibili potrebbe essere evitata attuando una gestione più consapevole dei dati. Di seguito vengono illustrati due casi: nel primo le informazioni sono state pubblicate inconsapevolmente, mentre nel secondo sono stati trasmessi dati confidenziali a terzi senza l'autorizzazione necessaria.

[39] Spekulative Berechnungen öffnen eine Hintertür zum Informationsklau (ethz.ch); Speculative calculations open a backdoor to information theft (ethz.ch)

5.5.1 Metadati contenuti nei file pubblicati

Per le imprese e le istituzioni, le pagine web sono piattaforme centrali che servono a comunicare le informazioni all'esterno nonché renderle disponibili. Le informazioni interne contenute nei metadati dei file[40] possono diventare involontariamente pubbliche. In tal caso, persone estranee possono risalire ai nomi degli impiegati, ai nomi utente, agli indirizzi e-mail, alle strutture delle cartelle, ai software impiegati e ai relativi numeri di versione. In riferimento ai ciberattacchi, le informazioni relative alle versioni e alle applicazioni utilizzate sono particolarmente interessanti per gli aggressori, perché possono fornire loro indizi rivelatori su possibili vettori di attacco.

Il problema dei metadati è stato riscontrato anche nell'Amministrazione federale, dove sono state adottate misure appropriate per sensibilizzare i collaboratori.

Conclusione / raccomandazioni

Anzitutto le organizzazioni dovrebbero fare il punto della situazione e verificare la presenza di metadati in tutti i file pubblicati. Dopo l'eventuale pulizia, i file possono essere ripubblicati. Prima di trasmettere o pubblicare file è consigliabile pulirli secondo una procedura prestabilita. Anche i collaboratori devono essere sensibilizzati e formati di conseguenza.

5.5.2 Smaltimento dei dispositivi informatici e dei supporti di dati

Nel dicembre del 2022 i media hanno reso noto che la Direzione di giustizia del Cantone di Zurigo per diversi anni non ha smaltito correttamente i dispositivi di memorizzazione. Di conseguenza, dal 2006 al 2012 i dati sensibili non crittografati sono finiti nelle mani di criminali. I supporti di dati contenevano anche numeri di telefono e indirizzi segreti di procuratori federali e giudici, atti penali, perizie psicologiche nonché planimetrie degli edifici.[41]

Da un rapporto d'indagine esterno sugli incidenti è emerso inoltre che i collaboratori avevano creato copie di file in drive archiviati localmente per poter elaborare in modo più efficace i casi, poiché il sistema d'informazione giuridico si era rivelato inaffidabile. Questi drive archiviati localmente non erano però sufficientemente protetti, visto che i dati ivi contenuti non erano stati crittografati in maniera coerente.[42]

Conclusione / raccomandazioni

L'incidente mostra chiaramente che, con la progressiva digitalizzazione, alla sicurezza dei dati deve essere accordata la massima attenzione. A tal fine, i processi relativi a una conservazione sicura dei dati devono essere predisposti in maniera facilmente comprensibile per gli utenti, in modo tale che tutti i collaboratori rispettino le disposizioni.

---

40 I metadati (informazioni e caratteristiche relative ai file) sono contenuti in tutti i tipi di file. Mentre documenti nei formati quali Word o PDF possono presentare come metadati indicazioni sugli autori, i file fotografici includono anche campi di dati riguardanti la localizzazione (GPS).

41 Schweiz aktuell – Datenleck bei Justizdirektion Kanton Zürich: GPK stellt Antrag auf PUK (srf.ch)

42 Datenskandal Justizdirektion: Zürich setzt die Prioritäten falsch (nzz.ch)

I supporti di dati possono essere smaltiti i diversi modi, ossia mediante sovrascrittura dei dati, smagnetizzazione o distruzione fisica. Se affidate l'operazione di cancellazione a un fornitore di prestazioni esterno, sceglietelo con cura, selezionate una procedura adeguata e assicuratevi che il processo di distruzione dei dati (o del supporto di dati) sia registrato.

Sul sito dell'NCSC sono pubblicate alcune misure per le imprese in caso di fuga di dati.

5.6 Aggiornamento sulla guerra in Ucraina

5.6.1 Proseguimento delle attività nel ciberspazio senza successi degni di nota

Anche nel secondo semestre del 2022 la guerra in Ucraina continua a svolgere un ruolo centrale nel contesto geopolitico. L'ultimo rapporto semestrale ha evidenziato i principali ciberincidenti durante l'attuale conflitto in Ucraina e nel periodo precedente la crisi.[43] Da allora, non sono stati registrati cambiamenti significativi per quanto concerne i tipi di ciberattacchi, malgrado l'intensità degli stessi sia aumentata.[44] Il Servizio di sicurezza ucraino ha riferito che nel 2022 sono stati neutralizzati 4500 ciberattacchi, cioè il triplo rispetto all'anno precedente.[45] La Russia continua quindi a mettere sotto pressione l'Ucraina nel ciberspazio, tuttavia finora non ha conseguito grandi successi. Nell'ultimo rapporto semestrale sono state formulate tre ipotesi sul perché la Russia non lanci ciberattacchi distruttivi e riconoscibili:

1. la Russia mette a segno ciberattacchi distruttivi contro l'Ucraina, che tuttavia non sono resi pubblici proprio perché il conflitto è ancora in corso;
2. la Russia conduce ciberattacchi distruttivi contro l'Ucraina, ma quest'ultima riesce a difendersi bene anche grazie all'appoggio di altri Stati e di partner privati;
3. la Russia non conduce ciberattacchi distruttivi contro l'Ucraina, in particolare perché ritiene che l'impiego di mezzi militari convenzionali sia più idoneo a raggiungere determinati obiettivi.

Le informazioni finora disponibili sulle attività perpetrate nel ciberspazio correlate alla guerra in Ucraina mostrano che la seconda ipotesi è quella più verosimile. La Russia pare essere molto attiva. Dall'ottobre 2022 colpisce molto duramente le infrastrutture ucraine del settore dell'energia, senza tuttavia riportare successi nel ciberspazio perché l'Ucraina si sta difendendo bene.[46] I ciberattacchi non sono apparentemente considerati un'alternativa ai mezzi militari convenzionali, bensì sono spesso impiegati in contemporanea, esercitando così una certa influenza. La campagna sferrata contro le centrali elettriche ucraine tra ottobre e novembre 2022 è un esempio di quest'operazione pluridimensionale. Gli attacchi missilistici sono stati abbinati a ciberattacchi e ad attività propagandistiche. L'obiettivo dei ciberattacchi è esercitare maggiore pressione su un settore che già deve fare i conti con risorse limitate, alcune delle quali sono state distrutte dai mezzi militari convenzionali. Le attività propagandistiche

---

43 Rapporto semestrale 2022/1 (ncsc.admin.ch), n. 3

44 The number of cyberattacks on Ukraine keeps increasing (cip.gov.ua)

45 SSU neutralized over 4,500 cyberattacks on Ukraine in 2022 (ssu.gov.ua)

46 SSU neutralized hundreds of cyberattacks on Ukrainian cogeneration plants and energy companies in 2022 (ssu.gov.ua)

miravano a scaricare la responsabilità delle conseguenze degli attacchi (tra cui le interruzioni di corrente) sull'Ucraina, sui governi locali o sulle grandi imprese ucraine.[47] Tuttavia, le ciberoperazioni non hanno sortito l'effetto sperato poiché l'Ucraina era preparata. La ragione dell'insuccesso russo risiede nel fatto che non sono stati lanciati nuovi tipi di ciberattacchi, bensì si è agito secondo schemi già noti ed è stato quindi possibile sventarli tramite l'attuazione di strategie di difesa collaudate.[48]

5.6.2 Ciberattacchi diversi, conseguenze diverse

Sono stati pubblicati numerosi contributi su ciberattacchi compiuti nell'ambito del conflitto in Ucraina, anche da organi di stampa non specializzati. Purtroppo alcuni di questi contributi non specificano né il tipo né l'entità degli attacchi e non consentono quindi una visione differenziata dei fatti. La descrizione di alcuni ciberattacchi riportata nelle pagine successive intende esporre, a titolo di esempio, diverse conseguenze e sottolineare l'importanza di leggere in maniera avveduta gli articoli che utilizzano concetti non specifici.

5.6.2.1 Attacchi alla disponibilità (attacchi DDoS)

Gli attacchi DDoS sono stati la tipologia di ciberattacchi più visibili nel periodo di riferimento.[49] Essi mirano a rendere inaccessibili pagine web o altri servizi online, principalmente sovraccaricandoli con un numero elevato di richieste. Tali attacchi sono stati condotti soprattutto da gruppi di hacktivisti che si sono schierati con uno dei due belligeranti. I gruppi di hacktivisti filorussi come KillNet scelgono i bersagli e i Paesi target in base al sostegno che questi ultimi offrono all'Ucraina o alle sanzioni imposte alla Russia. Nel contesto della guerra in Ucraina, i danni causati dagli attacchi sono stati finora marginali e hanno leso principalmente la reputazione.

Ne è un esempio l'attacco DDoS ai siti web degli aeroporti negli Stati Uniti da parte di KillNet nell'ottobre del 2022[50], che ha comportato la temporanea interruzione della disponibilità di diversi siti web aeroportuali. I passeggeri non potevano, ad esempio, controllare lo stato del proprio volo. Tuttavia, gli attacchi non hanno avuto alcuna ripercussione sulle attività operative degli aeroporti coinvolti.

5.6.2.2 Diffusione di software dannosi

Nel periodo di riferimento sono state rese note numerose campagne che diffondevano software dannosi, rivolte specialmente a istituzioni ucraine.[51] L'intento era accedere ai sistemi infettandoli con malware. In guerra, tali intrusioni servono soprattutto a fare azioni di spionaggio (furto di informazioni) o di sabotaggio (interruzione del funzionamento dei sistemi). Spesso il software dannoso si cela in un'e-mail, che apparentemente proviene da uffici pubblici, incentrata su un tema di attualità. Il tema e il mittente dovrebbero indurre il destinatario a compiere un'azione necessaria per infettare il sistema target. Un altro modus operandi osservato è la

---

47 Cyber, Artillery, Propaganda. General overview of the dimensions of Russian aggression (cip.gov.ua); Preparing for a Russian cyber offensive against Ukraine this winter (microsoft.com)

48 Cyber, Artillery, Propaganda. General overview of the dimensions of Russian aggression (cip.gov.ua)

49 Timeline of Cyberattacks and Operations (cyberpeaceinstitute.org)

50 Coverage of Killnet DDoS attacks plays into attackers' hands, experts say (therecord.media)

51 Timeline of Cyberattacks and Operations (cyberpeaceinstitute.org)

creazione di siti web fasulli che assumono la veste di servizi ufficiali. Gli aggressori inseriscono i software dannosi all'interno di un programma che l'utente deve installare. Il malware può essere diffuso anche sfruttando le vulnerabilità di un sistema. In questo caso, di regola non è necessaria l'interazione dell'utente del sistema target. Gli effetti di tali campagne variano notevolmente e dipendono dal tipo di software dannoso e dal sistema infetto. Ad esempio, un malware che sottrae informazioni da un computer di uno studente avrà probabilmente conseguenze meno gravi rispetto a un malware che si insinua nel sistema di un ospedale e che ne perturba l'attività.

Ad esempio, nel luglio del 2022 tra i sistemi delle autorità ucraine era stato diffuso il malware GammaLoad. L'attacco è stato attribuito al gruppo russo «Advanced Persistent Threat» (APT) Gamaredon.[52] Il software dannoso GammaLoad è stato diffuso sotto forma di presunto foglio informativo allegato a e-mail che fingevano provenire dall'Accademia nazionale per i servizi di sicurezza dell'Ucraina. Una volta infettato il sistema target con GammaLoad, il gruppo succitato può estrapolare informazioni o propagare nel sistema altri malware con ulteriori funzioni, ad esempio a scopo di sabotaggio.

In un altro caso, nell'ottobre del 2022 tre aziende di trasporto e logistica attive in Ucraina e Polonia sono state infettate nel giro di poche ore dal ransomware Prestige, attribuito al gruppo russo APT Sandworm.[53] Un ciberincidente di questo tipo può compromettere le attività delle aziende colpite e, di conseguenza, anche il trasporto delle merci. Tuttavia, è stato possibile contenere i danni dell'attacco grazie a una pronta reazione.

5.6.3 Sviluppi futuri

Al momento nulla fa presagire una diminuzione delle attività nel ciberspazio legate alla guerra in Ucraina. Finché la situazione bellica perdura, la Russia continuerà probabilmente a lanciare attacchi di questa portata e a sfruttare qualsiasi opportunità per ottenere gli effetti auspicati in combinazione o meno con attività in altri settori operativi.

---

52 Кібератаки групи UAC-0010 (Armageddon) з використанням шкідливої програми GammaLoad.PS1 v2 (CERT-UA#5003,5013,5069,5071) (cert.gov.ua)

53 New "Prestige" ransomware impacts organizations in Ukraine and Poland (microsoft.com)