UNIVERSITÀ DI PAVIA
Area Sistemi Informativi

n 8 Maggio 2023

Attacchi informatici: le misure di difesa dell'Ateneo nell'ultimo mese

I tentativi di intrusione nei sistemi informatici o di raccolta illecita di informazioni sono un fenomeno da monitorare e fronteggiare quotidianamente in Ateneo.

Ad oggi non ci sono state perdite di dati grazie alle misure di protezione adottate che hanno ben anticipato le intenzioni malevole e messo al sicuro il lavoro interno svolto.

La sicurezza collettiva dipende molto anche dalla responsabilità del singolo nell'utilizzare i propri dispositivi, tenerli aggiornati e relazionarsi con l'Area Sistemi Informativi qualora non si senta adeguatamente protetto.

I numeri sotto riportati evidenziano infatti ancora margini di miglioramento nel comportamento di ciascuno di noi oltre alla necessità di un costante lavoro interno ad ogni struttura al fine di acquisire consapevolezza dei rischi e quindi di adottare comportamenti adeguati alle condizioni di sicurezza.

In questo mese abbiamo avuto 11 pc infetti che sono stati segnalati e bonificati e circa 245 comunicazioni C&C rilevate e bloccate oltre a 2 minacce Zero-Days bloccate.

Queste tipologie di attacchi rappresentano uno dei primi fenomeni da monitorare poiché potrebbero nascondere malware, cryptolocker o altri fenomeni malevoli che approfondiremo nei successivi numeri di questa newsletter.

In questo numero della newsletter relativa alla cybersecurity tratteremo della protezione degli account tramite l'adozione dell'autenticazione a due fattori (2FA)

Malware and Attacks

11
Computers Infected with Bots

245
Communications with C&C* Sites

* C&C - Command and Control.
If proxy is deployed, there might be additional infected computers.

6 Known Malware Downloaded by

18 Users

2 Zero-Days Downloaded

Zero-days downloaded present a unique count of old or new malware variant with un-known anti-virus signature.

222
Unique Software Vulnerabilities were Attempted to be Exploited

Indicates potential attacks on computers on your network.

High Risk Web Access

7
High Risk Web Applications

271.5MB

Potential risks: opens a backdoor to your network, hides user activity, causes data leakage or malware infections.

0
High Risk Web Sites

0 hits

Potential risks: Exposure to web-based threats and network infection. Examples: Spam, malicious, phishing web sites.

SaaS Applications

0
SAAS Applications Seen

1
Users Using SAAS Application

Applications that have integration with our Harmony Email & Collaboration solution and can be fully protected by our Threat Prevention engines.

Data Loss

0
potential data loss incidents

0
sensitive data categories

Indicates information sent outside the company or to unauthorized internal users. Information that might be sensitive. See GDPR Article 5

Autenticazione a Due Fattori (2FA) : perché è utile e come attivarla

Oggi non è più sufficiente proteggere i propri account con una password forte: è opportuno – anzi necessario – **utilizzare l'autenticazione forte (strong authentication)**, nota anche come **autenticazione a due fattori** (2FA: two factor authentication).

Le debolezze delle "semplici" password

È ormai noto quanto sia importante usare password molto complesse e sempre diverse, così come diventa indispensabile usare strumenti per riuscire a ricordare le tante password (e tutte differenti) che ci troviamo a gestire: impossibile riuscire a ricordale tutte. Per questo sono di grande aiuto i sistemi di "password manager", applicazioni dedicate a conservare tutte le nostre password in modo sicuro e – ovviamente – crittografato.

Ma anche se vengono messe in pratica le buone regole sopra descritte, non si può escludere che una password venga rubata o scoperta. Sono frequenti i casi di violazione di siti (data breach) con il furto massivo di migliaia o milioni di password: in questi casi le password finiscono nel mercato nero del web (dark web) e qualcuno potrebbe usarle.

Per rendersene conto potrebbe bastare una visita al sito **Have i been pwned?** (il cui nome si potrebbe tradurre con: "Sono stato violato?").

É stato realizzato dall'esperto australiano di cyber security Troy Hunt a fine 2013 e oggi contiene circa 9,5 miliardi di account violati (raccolti da tutti i data breach di cui si ha notizia).

Se uno username che utilizziamo per i nostri account è presente nell'elenco, dobbiamo essere consapevoli che assieme a quello username sarà associata qualche nostra password rubata.

Un'autenticazione basata solo su password è dunque intrinsecamente debole, anche se la password impostata è robusta, perché la sicurezza dell'account dipende da un solo fattore, ossia la password.

Per innalzare i livelli di sicurezza sono state introdotte perciò le tecniche di "strong authentication" o autenticazione a due o più fattori.

Che cos'è l'autenticazione a due fattori

Definita anche 2FA o MFA (Multi-Factor Authentication), **rappresenta un'ulteriore sicurezza** ed è oggi **il sistema di protezione più sicuro che abbiamo a disposizione** per proteggere i nostri account.

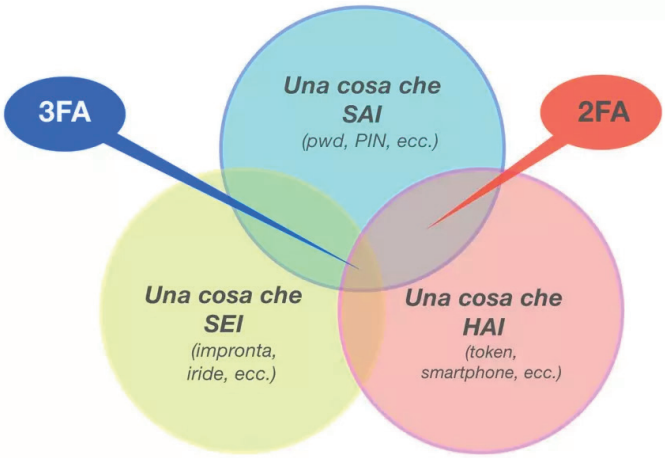
Come già anticipato, non può più essere considerata un "lusso" da applicare solo negli account bancari, ma **dovrebbe essere utilizzata** soprattutto per tutti quegli account – personali e aziendali – nei quali si trovano dati importanti. Quelli da proteggere con maggior attenzione sono gli account e-mail (se la nostra e-mail viene violata, tutta la nostra vita risulterà esposta), i servizi cloud e qualsiasi account aziendale.

Ormai tutti i siti importanti rendono disponibile l'autenticazione a due fattori in forma

facoltativa (quindi da attivare come opzione aggiuntiva).

Per accedere a qualunque sistema digitale (computer, bancomat, siti web o altro) occorrerà dapprima "presentarci" inserendo il nostro username. Poi dovremo "dimostrare" che siamo proprio noi: questa è la fase di "autenticazione" che può avvenire in tre diversi modi:

1. **Conoscenza:** "Una cosa che sai", per esempio una password o il PIN.
2. **Possesso:** "Una cosa che hai", come uno smartphone o un token di sicurezza (quelle piccole "chiavette" che ci davano le banche e che generavano un codice a 6 cifre).
3. **Inerenza:** "Una cosa che sei", come l'impronta digitale, il timbro vocale, il viso, l'iride, o un qualunque altro dato biometrico.



In molti casi l'autenticazione avviene con la sola password: si tratta di autenticazione ad un fattore.

Si parla invece di 2FA se si usano **almeno due dei tre fattori** sopra elencati. Ma non basta: la condizione affinché si possa definire "autenticazione a due fattori" si verifica solo quando i due fattori utilizzati sono di matrice differente: in altre parole se, per esempio, si usa "Una cosa che sai" + "Una cosa che hai".

Mentre **non può essere** – a rigore – **considerata 2FA un'autenticazione fatta con due password** (perché due fattori della stessa natura).

Esiste anche l'autenticazione a tre fattori (3FA), ovviamente se vengono richiesti tre fattori come l'autenticazione biometrica (impronta digitale, riconoscimento facciale o dell'iride)

Come funziona l'autenticazione a due fattori

Dopo aver inserito la password (primo fattore) del proprio account, **sarà richiesto di digitare un secondo fattore**, che nella maggior parte dei casi è un codice numerico. Questo secondo fattore in genere **viene ottenuto attraverso lo smartphone** (sotto forma di sms o tramite un'apposita applicazione) **o tramite un token fisico**.

A differenza della password, **il secondo codice è di fatto inattaccabile, perché generato in maniera pseudocasuale** secondo uno specifico algoritmo **ed ha una durata molto limitata nel tempo** (solitamente 30 secondi). **Per questo motivo, lo si definisce anche OTP: "One Time Password".**

Il secondo fattore può essere – in alternativa – di tipo biometrico ("una cosa che sei"). Ad esempio nelle applicazioni per smartphone fornite dalle banche: per aprire l'app e anche per eseguire operazioni dispositive (ad esempio: fare un bonifico), viene richie-

sta la seconda autenticazione con l'impronta digitale o con il riconoscimento facciale.

Come ottenere il secondo fattore di autenticazione di tipo numerico

Il secondo fattore in forma numerica (One Time Password) è la soluzione più frequentemente usata nella 2FA.

Vi sono modalità differenti per ottenerlo:

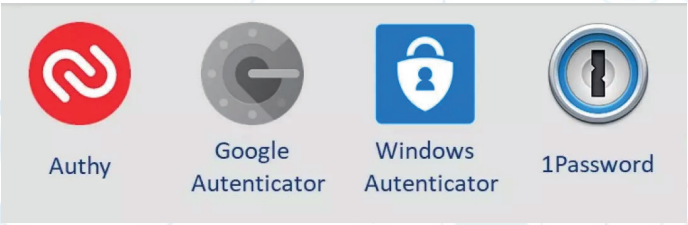
OTP con Sms

Attraverso un SMS inviato sul nostro smartphone: è una **modalità molto diffusa, ma è indiscutibilmente la meno sicura**. Ciò a causa della ormai nota vulnerabilità del protocollo Signalling System No 7 (SS7). Ma il vero motivo che rende sconsigliabile questo metodo è soprattutto un altro: la truffa ormai frequente e conosciuta come **SIM Swap Fraud**. In pratica, un malintenzionato può riuscire a trasferire da una SIM card a un'altra il nostro numero di telefono. Portare a termine un'operazione di SIM swapping illegittima significa ottenere il completo accesso al numero di telefono del legittimo (e ignaro) proprietario di tale numero. Soprattutto permette di ricevere l'SMS con i codici di autenticazione a due fattori, ovviamente per realizzare operazioni bancarie.

Il proprietario dello smartphone si troverà con il dispositivo muto e disconnesso dalla rete. Quando si sarà reso conto che la sua SIM non è più attiva potrebbe essere troppo tardi ed i soldi già scomparsi dal suo conto corrente.

Applicazioni dedicate per ottenere gli OTP

Quando il sito rende disponibile questa opzione è consigliabile sceglierla, perché è **il metodo più pratico**, non richiede la copertura telefonica ed è sicuro. Tali applicazioni sono definite **"Soft Token"**: in pratica si comportano esattamente come i token hardware che venivano forniti dalle banche: generano un OTP a 6 cifre, associato ad uno specifico account.



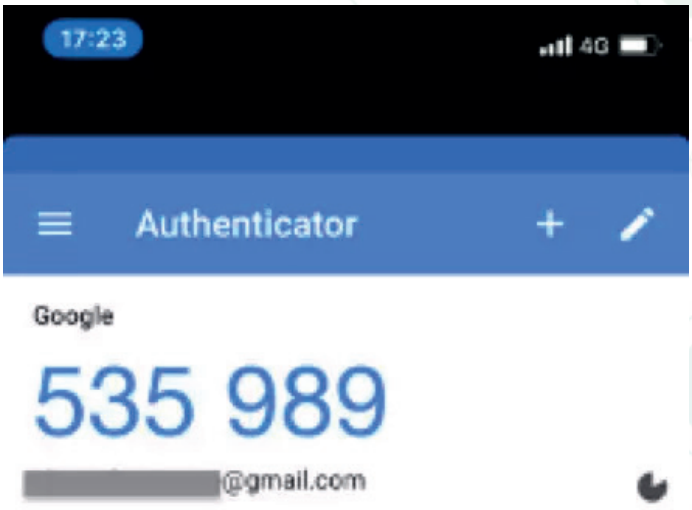
Esistono numerose applicazioni del genere: le più note – tutte gratuite – sono **Authy, Google Authenticator, Microsoft Authenticator**. Anche i migliori **password manager offrono questa funzionalità**.

Come attivare l'autenticazione a due fattori

La modalità di attivazione dell'autenticazione a due fattori è – in pratica – sempre la stessa: dopo aver effettuato la registrazione sul sito, si accede alla pagina delle "Impostazioni di Sicurezza" (il nome può anche essere leggermente diverso, ma si tratta sempre della sezione dove andiamo, per esempio, per modificare la password).

Si sceglie di attivare la 2FA, dopodiché **il sito chiederà in che modo vogliamo ricevere il codice**: il metodo più diffuso in tutti i siti è attraverso un SMS, quindi dovremo indicare uno **smartphone "affidabile"** al quale verrà inviato il codice.

Alcuni siti permettono di scegliere, in alternativa al codice via SMS, l'uso delle succitate applicazioni (soft token) in grado di generare il codice temporaneo (OTP). Come detto, se disponibile, è la scelta preferibile: in questo caso l'abbinamento viene fatto attraverso la lettura di un QRcode che compare sullo schermo del computer e che dovrà essere inquadrato con la camera dello smartphone, sul quale è stata preventivamente aperta l'applicazione.



Nella fase di attivazione dell'autenticazione a due fattori in genere (ma ogni sito potrebbe avere comportamenti differenti) verrà fornita anche una **chiave di recupero** (molto complessa, da conservare a parte).

Di regola per la 2FA si usano Password + Codice OTP, la chiave di recupero è la "soluzione di emergenza" da utilizzare solo in caso di: password dimenticata o dispositivo smarrito o rubato.

Esiste – quasi in tutti i siti – una comoda opzione che permetterà di non dover più inserire nei login successivi il codice OTP: questa opzione si chiama in genere: "considera questo dispositivo attendibile" (o qualcosa di simile) e va attivata una tantum.

In pratica, poiché l'autenticazione a due fattori è finalizzata ad evitare accessi da computer o dispositivi diversi dai nostri, si può fare in modo che il sito riconosca che si sta facendo il login dal dispositivo "abituale" e non venga più richiesto il secondo fattore di autenticazione.

I servizi che offrono l'autenticazione a due fattori

Ad eccezione dei servizi di internet banking, che lo impongono, in tutti gli altri siti **non si è obbligati ad usare l'autenticazione a due fattori**.

È un'opzione facoltativa, ma consigliata, almeno per i servizi più importanti quali, per esempio: Amazon, Apple ID (iCloud), Dropbox, Evernote, Facebook, Google, LinkedIn, Microsoft, PayPal, Twitter, Yahoo!, WordPress eccetera.

In pratica, **tutti i siti che gestiscono carte di credito o informazioni sensibili la rendono disponibile** (ed in molti casi la consigliano).

Sul sito Two Factor Auth (https://2fa.directory/it/) si può consultare l'elenco completo delle centinaia di siti ove è possibile attivarla, suddivisi per categorie. Inoltre, per ogni sito sono indicate le opzioni disponibili (SMS, hard token, soft token ecc.).

Un ulteriore vantaggio derivante dall'uso della 2FA: se attivata, non verranno più chieste le domande di sicurezza.

Autenticazione a due fattori: le indicazioni del NIST

Sono reperibile utili indicazioni sull'uso dell'autenticazione a due fattori anche nelle

linee guida emesse dal NIST.

il **NIST (National Institute of Standards and Technology)** è un'agenzia del governo degli Stati Uniti d'America che si occupa della gestione delle tecnologie. Fa parte del DoC, Department of Commerce (Ministero del Commercio).

Il NIST è nato nel 1901 ed ha come compito istituzionale quello di sviluppare standard tecnologici. In particolare, pubblica i Federal Information Processing Standard (FIPS), che definiscono gli standard obbligatori del governo statunitense.

Ovviamente gli standard definiti dal NIST non sono cogenti in Europa, tuttavia per la loro autorevolezza sono considerati un punto di riferimento a livello non solo USA, ma in tutto il mondo.

Il NIST tratta dell'uso delle password e dell'autenticazione a due fattori nella **SP 800-63** ed in particolare nella **SP 800-63-3 "Digital Identity Guidelines"**, disponibile a questo link: e nella **SP 800-63B "Digital Identity Guidelines – Authentication and Lifecycle Management"**.

Nella SP 800-63-3 la tabella 5.2 definisce i tre livelli **AAL (Authenticator Assurance Level)**, mentre al paragrafo 6.2 "Selecting AAL" vengono indicate le modalità per selezionare i livelli di autenticazione più appropriati per ogni tipo di servizio digitale.

I livelli AAL 2 e 3 richiedono l'uso dell'autenticazione forte a più fattori.

Nella SP 800-63B vengono esaminate le varie modalità disponibili per l'autenticazione a due fattori. Al cap. 4.2 viene illustrata la AAL 2, mentre al cap. 4.3 si tratta la AAL 3.

Viene stabilito che quando si usa una combinazione di due fattori di autenticazione, uno deve essere un segreto memorizzato, cioè una password (capitolo 5.1.1), mentre il secondo autenticatore deve essere basato sul possesso (cioè "qualcosa che hai"). Quindi il richiedente (colui che fa il login) deve dimostrare il possesso e il controllo di due distinti fattori di autenticazione, che abbiano il requisito di "garantire una resistenza all'impersonificazione" (in altre parole: impedire che qualcuno li possa usare al nostro posto).

Al successivo capitolo 5.1.3 Out-of-Band Devices viene deprecato l'utilizzo della linea telefonica per ricevere il secondo fattore OTP, proprio per il rischio di SIM swap (di cui abbiamo parlato in precedenza).

Viene invece consigliato l'utilizzo di un **"Multi-Factor OTP Device"**, come spiegato al cap. 5.1.5: potrebbe trattarsi anche di uno smartphone ("una cosa che hai"), che attraverso un'applicazione apposita genere un codice OTP "time-based"(come precedentemente spiegato).

Qui si evidenzia un aspetto molto importante: per maggior sicurezza lo smartphone deve essere preventivamente attivato da "qualcosa che sai" (una password di sblocco) oppure da "qualcosa che sei" (l'impronta digitale, la faccia, ecc.).

Quest'ultimo non è un passaggio da sottovalutare e fa capire perché, con l'entrata in vigore della Direttiva (UE) 2015/2366 (PSD2) non sono più ammessi i token hardware (le chiavette in plastica che generavano un codice a 6 numeri) per l'autenticazione

nei siti bancari: erano dispositivi non sicuri, dal momento che potevano essere attivati senza alcun codice di sicurezza. Quindi in caso di furto o smarrimento, chiunque avrebbe potuto utilizzarli.

La Strong Customer Authentication (SCA) nel mondo bancario

Sono state le banche ad introdurre per prime l'autenticazione a più fattori.

Ma recentemente questa è stata rivista e potenziata per effetto della Direttiva (UE) 2015/2366 nota come PSD2 (Payment Services Directive 2).

Tale direttiva dell'Unione Europea è stata recepita dall'Italia con il D.Lgs. 15 dicembre 2017, n. 218 e sostituisce la precedente Direttiva 2007/64/CE (c.d. Payment Services Directive).

La PSD2 è ora in vigore in tutti gli stati dell'Unione Europea, a seguito dell'adozione del Regolamento delegato (UE) 2018/389 pubblicato il 27 novembre 2017. In quanto Regolamento questo è obbligatorio e direttamente applicabile in ciascuno degli Stati membri dal 14 settembre 2019 (come specificato in art.38).

Questa direttiva affronta in modo importante l'autenticazione a più fattori, che viene definita Strong Customer Authentication (SCA). Ora è stata regolamentata in modo più forte e resa obbligatoria per le operazioni bancarie online (via internet e mobile).

Viene definita in modo molto preciso nella PSD2 all'art.4 comma 30 come:

«autenticazione forte del cliente»: *un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione.*

Le condizioni nelle quali deve essere obbligatoriamente applicata sono definite all'art. 97:

"Gli Stati membri provvedono a che un prestatore di servizi di pagamento applichi l'autenticazione forte del cliente quando il pagatore:

1. accede al suo conto di pagamento on line;
2. dispone un'operazione di pagamento elettronico;
3. effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi".

L'art. 74 stabilisce le responsabilità del pagatore e quelle del "prestatore di servizi di pagamento" (PSP: payment service provider). Quest'ultimo viene obbligato ad esigere un'autenticazione forte. In particolare (comma 2): "Se il prestatore di servizi di pagamento del pagatore non esige un'autenticazione forte del cliente, il pagatore non sopporta alcuna conseguenza finanziaria salvo qualora abbia agito in modo fraudolento. Qualora non accettino un'autenticazione forte del cliente, il beneficiario o il suo prestatore di servizi di pagamento rimborsano il danno finanziario causato al presta-

tore di servizi di pagamento del pagatore".

Concludiamo l'esame della PSD2 citando l'art. 98: questo assegna ad EBA (European Banking Authority) il compito di emanare le "Norme tecniche di regolamentazione in materia di autenticazione e comunicazione".

EBA ha rilasciato le **Regulatory Technical Standards (RTS)**, adottate il 27 novembre 2017 dalla Commissione Europea con il regolamento delegato (UE) 2018/389 e quindi cogenti dal 14 settembre 2019.

Le RTS specificano appunto i requisiti delle procedure di autenticazione forte (SCA) e le relative esenzioni d'uso, nonché i requisiti per la protezione delle credenziali di sicurezza degli utenti.

Senza entrare nel dettaglio delle RTS, si può comunque affermare che **le regole di sicurezza per la SCA** sono – in pratica – **quelle che illustrate nei punti precedenti**.

Per saperne di più...

- per informazioni: **https://trasformazionedigitale.unipv.it**
- per contattare l'Area Sistemi Informativi: **https://sos.unipv.it**
- se sei uno studente scrivi a questo indirizzo: **smart@ unipv.it** oppure contatta un tecnico del tuo dipartimento per ottenere informazioni
- informazioni in tempo reale su attacchi informatici: **https://www.csirt.gov.it**

Fonti

- Wikipedia portale sicurezza informatica - "*Autenticazione a due fattori*"
- NIST.gov - *SP 800-63-3 "Digital Identity Guidelines"*
- CSIRT.gov.it - *SP 800-63-3 "Autenticazione a più Fattori (Multi Factor Authentication – MFA)"*