UNIVERSITÀ DI PAVIA
Area Sistemi Informativi

n 11 Agosto-Settembre 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 12 pc infetti che sono stati segnalati e bonificati e circa 1700 comunicazioni C&C rilevate e 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 delle tecniche di difesa durante il "telelavoro".

Malware and Attacks

12
Computers Infected with Bots

1.7K
Communications with C&C* Sites

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

3 Known Malware Downloaded by

29 Users

2 Zero-Days Downloaded

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

181
Unique Software Vulnerabilities were Attempted to be Exploited

Indicates potential attacks on computers on your network.

High Risk Web Access

8
High Risk Web Applications

27.6MB

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

2
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

Tecniche di difesa per il “telelavoro”.

Negli ultimi tempi, c’è stato un maggior utilizzo del telelavoro e dello smartworking, anche dovuto all’emergenza COVID-19. Questo approccio lavorativo consente ai dipendenti di organizzazioni pubbliche e private, di svolgere le proprie mansioni da remoto, sfruttando le tecnologie digitali. Queste modalità hanno permesso di bilanciare meglio gli impegni personali con le richieste lavorative dell’organizzazione di appartenenza.

Tuttavia, va sottolineato che queste modalità di lavoro, specialmente quando implementata senza una formazione adeguata, comporta un aumento dei rischi legati alla sicurezza informatica. Questo perché i potenziali aggressori possono sfruttare l’espansione delle superfici di attacco dovute al lavoro da remoto per compiere attacchi informatici, sfruttando vulnerabilità nelle soluzioni tecnologiche impiegate.

Per garantire una gestione sicura delle operazioni ICT, è essenziale adottare buone pratiche. È di fondamentale importanza che le organizzazioni prendano precauzioni e mettano in atto misure di sicurezza per proteggere l’accesso remoto a tutte le risorse lavorative, al fine di mitigare i rischi cibernetici come violazioni dei dati, ransomware e defacement.

L’obiettivo di questa guida è fornire indicazioni di sicurezza per i modelli di lavoro agile. Essa offre raccomandazioni su come mantenere un alto livello di vigilanza e attuare adeguate misure di sicurezza informatica, al fine di contrastare efficacemente i rischi cibernetici.

Uso consapevole e sicuro dei dispositivi e degli strumenti da parte dei dipendenti.

Favorire la consapevolezza del personale riguardo all’utilizzo sicuro dei dispositivi e degli strumenti utilizzati per il lavoro da luoghi remoti, avviando anche la diffusione di direttive che includono:

- Fornire raccomandazioni ossia principi di buona condotta agli utenti lavoratori
- Elementi connessi all’impiego dei servizi informatici che supportano il lavoro agile, con particolare attenzione a quelli offerti da provider di servizi cloud. Questo può comprendere la regolamentazione dell’utilizzo sicuro di webcam e microfoni, oltre a definire il tipo di attività idonee da svolgere.

Accesso sicuro alla rete dell’organizzazione.

Tenere traccia del personale sia interno che esterno, come consulenti, ai quali è autorizzato il lavoro in modalità remota, ponendo attenzione nell’identificare gli utenti con

privilegi di accesso alle infrastrutture (amministratori) o ai dati (incaricati di gestione e del trattamento), e implementando misure di sicurezza “enforced” in base ai differenti livelli di accesso autorizzati.

Consentire l’accesso alla rete dell’organizzazione esclusivamente attraverso:

- Una VPN (Virtual Private Network) o tecnologie analoghe.
- Procedure di autenticazione robuste, come l’autenticazione a più fattori e/o l’utilizzo di one-time password (OTP).
- Utilizzo di vAPP (virtual Application), interfaccia desktop virtuale personale (VDI) o protocollo Remote Desktop Protocol (RDP) per accedere a desktop assegnati in sede.

Personalizzare le modalità di accesso in base alle categorie di utenti, ad esempio:

- Impiego di vAPP tramite browser per il personale non tecnico che usufruisce di webconsole o altri servizi accessibili via browser.
- Impiego di vAPP con RDP per accedere alla postazione di lavoro abituale o alla VDI dedicata per il personale tecnico che utilizza frequentemente più sistemi per configurazioni e gestione degli incidenti, ecc.

Garantire la protezione dei servizi accessibili all’interno della rete aziendale, ad esempio tramite l’implementazione di credenziali di accesso personali gestite attraverso appositi sistemi di sicurezza.

Adeguata sicurezza dei dispositivi.

Aggiornare frequentemente i dispositivi e i software, soprattutto dal punto di vista della sicurezza, ad es. con anti-malware. Inoltre, applicare tecniche di “hardening”, ovvero compiere una serie di configurazioni sui dispositivi e software allo scopo di minimizzare le vulnerabilità e i potenziali impatti di un attacco.

Configurare le vAPP in modo da prevenire qualsiasi tipo di accesso alle periferiche locali (ad es. porte USB) del sistema utilizzato per la connessione.

Se possibile e in base a un’analisi dei rischi appropriata, adottare strumenti per la cosiddetta “Endpoint Detection and Response” (EDR), che consentono di individuare e rispondere a eventuali minacce agli endpoint, ossia i dispositivi finali utilizzati nella rete.

Registrare in modo accurato gli accessi e le attività effettuate, mediante l’utilizzo di strumenti di virtualizzazione e di sistema. Questo approccio riveste un’importanza particolare nei confronti dei server e delle basi di dati, includendo il tracciamento degli accessi diretti.

Adeguata sicurezza della rete.

Effettuare controlli accurati per garantire che i dispositivi fisici e virtuali posti ai margini del sistema (come firewall, proxy, ecc.) siano configurati in modo adeguato e siano mantenuti aggiornati. Questo vale altresì per i dispositivi di rete come i router.

Quando possibile e basandosi su un’analisi dettagliata dei rischi, considerare l’implementazione di soluzioni volte a prevenire attacchi di tipo Distributed Denial of Servi-

ce (DDoS), prestando particolare attenzione alla protezione dei punti terminali delle connessioni VPN. In aggiunta, considerare l'adozione di sistemi per rilevare eventuali accessi non autorizzati (IDS - Intrusion Detection Systems).

Adeguata sicurezza del cloud.

Accertarsi che il fornitore di servizi cloud aderisca a diverse pratiche chiave, tra cui:

- Eseguire gli adempimenti richiesti in conformità agli obblighi relativi alla sicurezza cibernetica e al trattamento dei dati personali, come previsto dal GDPR (Regolamento Generale sulla Protezione dei Dati).
- Adottare protocolli crittografati e meccanismi di autenticazione robusta nell'ambito dei servizi forniti, al fine di assicurare una protezione adeguata.
- Garantire un elevato livello di sicurezza informatica che rispetti gli standard sia nazionali che internazionali riconosciuti.
- Implementare politiche adeguate per la protezione dei dati dell'organizzazione, comprendenti aspetti come l'utilizzo di crittografia per i dati memorizzati e il diritto all'oblio.

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 - *Telelavoro*
- CSIRT Italia