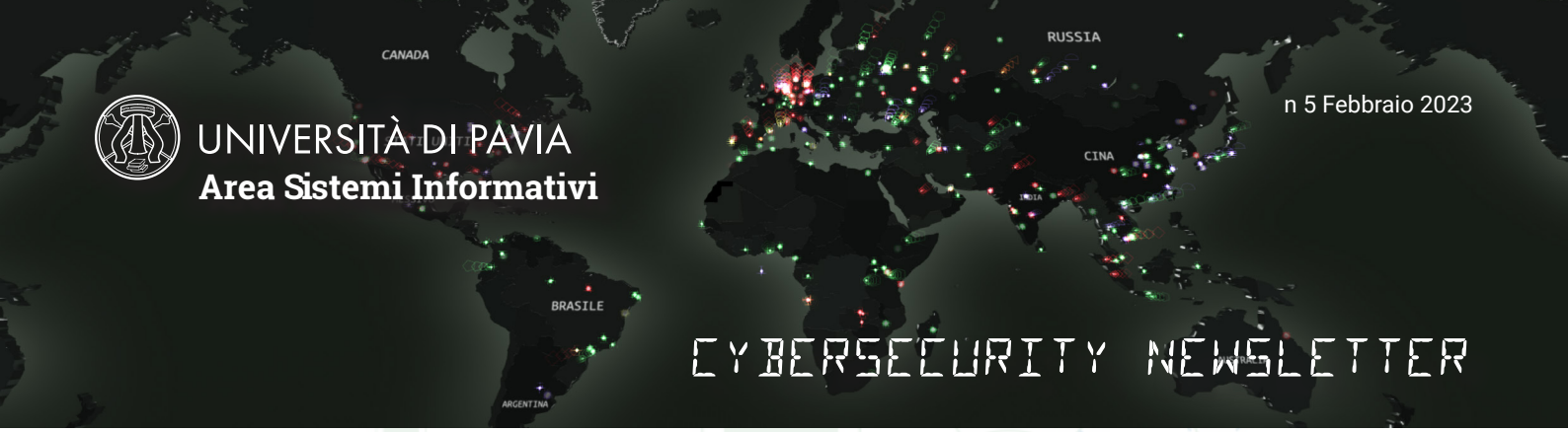


UNIVERSITÀ DI PAVIA
Area Sistemi Informativi

n 5 Febbraio 2023

CYBERSECURITY NEWSLETTER

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 94 pc infetti che sono stati segnalati e bonificati e circa 49.100 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 quarto numero della newsletter relativa alla cybersecurity affronteremo il tema dei "firewall"

Malware and Attacks

94
computers infected with bots

49.1K
communications with C&C* sites

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

2 known malware downloaded by

157 users

2 Zero-days downloaded

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

304
unique software vulnerabilities were attempted to be exploited

Indicates potential attacks on computers on your network.

High Risk Web Access

12
high risk web applications

46.2MB

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

1
high risk web sites

15 hits

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

0
cloud applications

0B

Risk of data loss and compliance violations. Examples: Dropbox, Google Drive, OneDrive.

Data Loss

0
potential data loss incidents

0
sensitive data categories

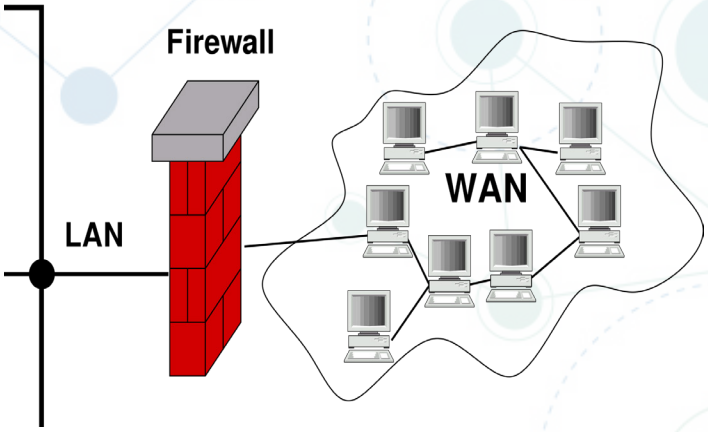
Indicates information sent outside the company or to unauthorized internal users. Information that might be sensitive. See GDPR Article 5

Firewall: che cos'è

Un firewall è un dispositivo per la sicurezza della rete che permette di monitorare il traffico in entrata e in uscita utilizzando una serie predefinita di regole per consentire o bloccare gli eventi. Un firewall può essere costituito da un componente hardware, da un componente software o da entrambi. Sono strumenti che costituiscono una barriera tra le reti interne e le reti esterne come Internet.

Con la nascita delle reti LAN e l'aumentare della connettività tra le stesse, favorita anche dalla diffusione dei primi router, cominciarono a emergere i primi problemi di sicurezza riguardanti soprattutto gli accessi non autorizzati. Una delle prime soluzioni adottate consisteva nell'impostare all'interno dei router stessi le liste di controllo degli accessi (ACL) che consentivano di stabilire quali pacchetti accettare o scartare sulla base dell'indirizzo IP. Questo approccio diventò sempre meno utilizzabile quanto più aumentavano i dispositivi connessi alla rete Internet. Per cercare di contrastare le intrusioni, alla fine degli anni 1980 vennero introdotti i primi firewall.

La prima generazione fu quella dei "packet filter firewall" o "stateless firewall", il cui primo esemplare venne sviluppato nel 1988 dalla Digital Equipment Corporation. Il loro funzionamento consiste nel filtrare il traffico secondo un insieme di regole basate su alcune informazioni presenti nell'header dei pacchetti. Questi semplici filtri però possono essere aggirati mediante la tecnica nota come "IP spoofing", una tipologia di attacco informatico che utilizza un pacchetto IP nel quale viene falsificato l'indirizzo IP del mittente. Nell'header di un pacchetto IP si trova, infatti, uno specifico campo, il Source Address, il cui valore indica l'indirizzo IP del mittente: modificando questo campo si può far credere che un pacchetto IP sia stato trasmesso da una macchina host diversa.
La seconda generazione di firewall introdusse, rispetto alla prima, la possibilità di salvare e monitorare lo stato di una connessione. Il primo "stateful firewall" venne sviluppato tra il 1989 e il 1990 dagli AT&T Bell Laboratories. Questa tipologia di firewall consente la formulazione di regole in grado di bloccare pacchetti fasulli, cioè non appartenenti ad alcuna connessione attiva.



La crescita di Internet portò alla diffusione di nuove tipologie di attacchi ai quali gli stateful firewall non erano in grado di far fronte. Infatti i firewall della seconda generazione, come quelli della prima, non avevano la capacità di individuare le minacce all'interno del traffico in quanto riuscivano a classificarlo semplicemente sulla base della porta e del protocollo. Per fronteggiare tale problematica fu sviluppato l'application firewall (anche detti proxy firewall o application gateway), una nuova generazione di firewall in grado di

offrire protezione fino al livello applicativo (livello 7) del modello OSI.
Nella seconda metà degli anni 2000 vennero realizzati i primi NextGeneration-Firewall (NGFW) che riunivano vecchie e nuove tecnologie di sicurezza in un'unica soluzione, con caratteristiche migliorative sia prestazionali che di gestione.

Un firewall può essere sia un software oppure una combinazione di hardware e software, in particolare si definisce "firewall appliance" nel caso in cui sia realizzato come un dispositivo hardware provvisto di software integrato in grado di svolgere le funzioni di firewall.
Lo scopo del firewall è controllare gli accessi alle risorse di un sistema filtrando tutto il traffico che tale sistema scambia con l'esterno: il sistema può essere un singolo computer o una rete di computer (detta rete interna o rete locale o rete privata) mentre l'ambiente esterno con cui interagisce è tipicamente una rete che si suppone sconosciuta, insicura e non attendibile (detta rete esterna o rete pubblica). In particolare un firewall filtra il traffico sulla base di un insieme di regole, solitamente dette policy che vengono applicate secondo due possibili criteri generali:

criterio "default-deny": viene permesso solo ciò che viene dichiarato esplicitamente e tutto il resto viene vietato;
criterio "default-allow": viene vietato solo ciò che è esplicitamente proibito e il resto viene permesso.

I firewall utilizzano normalmente il criterio "default-deny" poiché garantisce una maggiore sicurezza e una maggiore precisione nella definizione delle regole rispetto al criterio "default-allow", anche se quest'ultimo consente una configurazione più semplice. L'analisi dei pacchetti che costituiscono il traffico, secondo i criteri di sicurezza formalizzati dalle regole, si traduce in una delle seguenti azioni:

allow: il firewall lascia passare il pacchetto;
deny: il firewall blocca il pacchetto e lo rimanda al mittente;
drop: il firewall blocca il pacchetto e lo scarta senza inviare alcuna segnalazione al mittente.

I firewall in generale si dividono in "host-based" e "network-based" a seconda della natura del sistema che proteggono. Un "host-based" firewall, chiamato anche personal firewall o firewall software, è un'applicazione software che controlla il traffico uscente ed entrante da un singolo computer. In particolare blocca le applicazioni installate sulla macchina a cui non è concessa la connessione con l'esterno. Un "network-based firewall", detto anche network firewall o firewall hardware, è un componente hardware standalone che viene posto sul confine di una rete in modo da filtrare tutto il traffico che questa scambia con l'esterno (detto anche firewall perimetrale).

I firewall hardware sono macchine progettate per la particolare funzione che devono svolgere e possono essere realizzate con hardware e software dedicati o con un server opportunamente configurato per eseguire esclusivamente la funzionalità di firewall. Sono dotati di più schede di rete e presentano un sistema operativo minimale

composto solo da software indispensabile per l'esecuzione del firewall. Per questo motivo i firewall hardware sono più sicuri e allo stesso tempo più complessi da configurare rispetto ai firewall software.

Filtraggio dei contenuti

Un'altra funzione prevista è la possibilità di filtrare l'accesso ai siti per categorie, o in base all'URL presente in liste di riferimento nel database del firewall stesso, esempio:

- contenuti non adatti ai minori;
- contenuti ritenuti non pertinenti con l'attività lavorativa (in una rete aziendale);

Altre funzionalità associate (NAT e Intrusion Prevention System)

Una funzione spesso associata al firewall è quella di NAT (Network Address Translation), che contribuisce a rafforzare la sicurezza dei computer interni mascherandone gli indirizzi IP.
Per implementare il NAT il firewall ha necessità di effettuare il tracciamento delle connessioni, ovvero di tenere traccia di tutte le connessioni che lo attraversano. Per "connessione" in questo contesto si intende un flusso bidirezionale di pacchetti tra due endpoint.
I firewall possono registrare tutte le operazioni fatte (logging), effettuare registrazioni più o meno selettive (ad esempio, registrare solo i pacchetti che violano una certa regola, registrare solo un numero di pacchetti al secondo oppure tenere statistiche di quali regole sono state più violate.

Limiti

Il firewall, pur essendo spesso un componente vitale in una strategia di sicurezza informatica, resta un singolo elemento di tale strategia:

- la sua efficacia è legata strettamente all'efficacia delle regole con cui è stato configurato (es. regole permissive possono lasciare falle di sicurezza);
- la sua configurazione è un compromesso tra usabilità della rete, sicurezza e risorse disponibili per la manutenzione della configurazione stessa (le esigenze di una rete cambiano rapidamente);
- una quota rilevante delle minacce alla sicurezza informatica proviene dalla rete interna (portatili, virus, connessioni abusive alla rete, accessi VPN, reti wireless non adeguatamente protette).

Tipologie

Generalmente classificati come firewall di rete o firewall host.
I primi sono normalmente posizionati tra la intranet e la WAN, si tratta normalmente di appliance che possono offrire anche funzionalità aggiuntive alla rete interna che proteggono, come ad es. un servizio DHCP o VPN.

La seconda tipologia di firewall, definito “Personal Firewall”, si installa direttamente sui sistemi da proteggere, ne controlla le comunicazioni in entrata e in uscita dal sistema stesso, permettendo o vietando alcuni tipi di comunicazione in base a regole o policy di sicurezza preimpostate dall’utente in fase di configurazione
Rispetto ad un firewall perimetrale, il personal firewall è eseguito sul sistema che dovrebbe proteggere, ed è quindi soggetto al rischio di venir disabilitato da un malware che prenda il controllo del computer. Inoltre, la sua configurazione è spesso lasciata a utenti finali poco esperti.

Packet Filter Firewall o Stateless Firewall. Un packet filter firewall o stateless firewall analizza ogni pacchetto che lo attraversa singolarmente, senza correlazione con i pacchetti che lo hanno preceduto. In tale analisi vengono considerate solo alcune informazioni contenute nell’header del pacchetto, ossia l’indirizzo IP della sorgente, l’indirizzo IP della destinazione, la porta tcp/udp della sorgente, la porta tcp/udp della destinazione e il protocollo di trasporto. Su questi parametri vengono costruite le regole che formalizzano la policy del firewall e che stabiliscono quali pacchetti lasciar passare e quali bloccare. Questo tipo di filtraggio è semplice e leggero ma non garantisce un’elevata sicurezza. Infatti risulta vulnerabile ad attacchi di tipo “IP spoofing” in quanto non distingue se un pacchetto appartiene o meno a una connessione attiva. Quindi, a causa della mancanza di stato, il firewall lascia passare anche i pacchetti il cui indirizzo IP sorgente originale, ad esempio non consentito dalla policy del firewall, viene volutamente modificato con un indirizzo consentito.

Stateful Firewall o Circuit-Level Gateway. Uno stateful firewall opera nella stessa modalità del firewall “packet filter” ma tiene traccia delle connessioni e del loro stato. Questa funzionalità, detta stateful inspection, viene implementata utilizzando una tabella di stato interna al firewall nella quale ogni connessione TCP e UDP viene rappresentata da due coppie di valori costituite da indirizzo IP e porta, una per ciascun endpoint della comunicazione. Per tenere traccia dello stato di una connessione TCP vengono memorizzati il sequence number, l’acknowledgement number e i flag che ne indicano l’inizio (SYN), la parte centrale (ACK) e la fine (FIN) della connessione. Quindi uno stateful firewall bloccherà tutti i pacchetti che non appartengono ad una connessione attiva, a meno che non ne creino una nuova, o che non rispettino l’ordine normale dei flag nella comunicazione. La possibilità di filtrare i pacchetti sulla base dello stato delle connessioni previene gli attacchi di tipo IP spoofing ma comporta una maggiore difficoltà nella formulazione delle regole.

Application Firewall - Proxy Firewall - Application Gateway. Un application firewall o proxy firewall o application gateway opera fino al livello 7 del modello OSI filtrando tutto il traffico di una singola applicazione sulla base della conoscenza del suo protocollo. Questo tipo di firewall analizza i pacchetti nella sua interezza considerando anche il loro contenuto (payload) ed è quindi in grado di distinguere il traffico di un’applicazione indipendentemente dalla porta di comunicazione che questa utilizza. Un’altra caratteristica che lo distingue da un packet filter firewall e da uno stateful firewall è la capacità di spezzare la connessione tra un host della rete che protegge e un host della rete esterna. Infatti nelle comunicazioni svolge il ruolo di intermediario

ed è quindi l'unico punto della rete che comunica con l'esterno. Sebbene aumenti il livello della sicurezza, un application firewall è specifico per ogni applicazione e può costituire un collo di bottiglia per le performance della rete.

Next-Generation Firewall. Un next-generation firewall è una piattaforma che riunisce in un' unica soluzione diverse tecnologie per la sicurezza. Fra queste ci sono le tecnologie di filtraggio presentati in precedenza ovvero il filtraggio stateless, la stateful inspection, l'analisi dei pacchetti a livello applicativo (deep-packet inspection) e altre funzionalità aggiuntive come il NAT e il supporto alle VPN.
Un firewall di tipo NGFW deve inoltre avere integrata la funzionalità di preventione delle intrusioni, il riconoscimento e controllo delle applicazioni per individuare e bloccare le app pericolose e tecniche per far fronte alle minacce alla sicurezza.

Definizioni

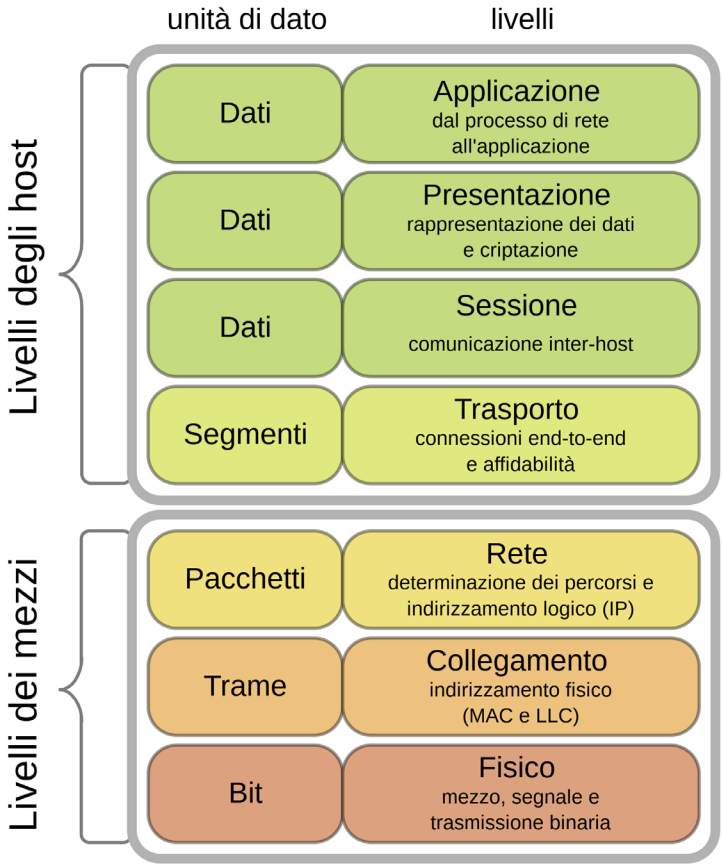
LAN: Local Area Network - Sistema di rete che permette ad apparecchiature di comunicare tra loro in un'area delimitata, senza attraversamento di spazi pubblici, utilizzando un canale fisico a elevata velocità e basso tasso di errore

MAN: Metropolitan Area Network - Sistema di rete che si estende in ambito urbano

WAN: Wide Area Network - Sistema di comunicazione che si estende su un'area geografica

DMZ: Demilitarized Zone - Sottorete fisica o logica che contiene ed espone dei servizi ad una rete esterna non ritenuta sicura

Modello OSI - Open Systems Interconnection, conosciuto anche come modello ISO/OSI, in telecomunicazioni e in informatica, è uno standard definito dall'International Organization for Standardization (ISO). Tale modello definisce l'architettura logica della rete, una struttura a strati composta da una pila di protocolli di comunicazione suddivisa in 7 livelli, che insieme eseguono tutte le funzionalità di rete seguendo un modello logico-gerarchico.



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 - *Firewall*
- Cisco - *Cos'è un firewall ?*