POLITICA DI FILTRO SUL TRAFFICO DI RETE

Approvazione
Data: **01/09/2023**
Dirigente ASI: **Dott.ssa Francesca Pruneti**
Firmato digitalmente ai sensi del D.Lgs. n. 82/2005

Informazioni sul documento		
Redazione a cura di: *U.O. Sicurezza IT* *U.O. Sistemi Tecnologici e Infrastrutture*	**Destinatari:** *Chiunque utilizzi dati, servizi e risorse informatiche dell'Università di Parma*	**Deposito del documento:** *www.unipr.it/regolamento-sicurezza-IT*

Sommario

1. Scopo del documento 3
2. Ambito di applicazione 3
3. Filtri sui flussi dati delle reti in cloud 3
4. Filtri sui flussi di dati delle reti interne 3

1. Scopo del documento

Lo scopo di questo documento è definire una politica di filtraggio dei dati, dei servizi e delle risorse informatiche di cui l'Università di Parma è titolare, con l'intento di aumentare la sicurezza informatica e proteggere la privacy.

2. Ambito di applicazione

La politica descritta in questo documento si applica agli scambi di dati che avvengono tra le reti, i dispositivi, le applicazioni, i servizi dell'Università di Parma verso Internet e tra di loro, sulla rete interna o nel cloud. Ogni flusso di dati che parte o arriva a delle risorse informatiche dell'Università di Parma, siano esse interne o cloud, è potenzialmente soggetto alle politiche di filtro descritte in questo documento.

3. Filtri sui flussi dati delle reti in cloud

La posta elettronica viene filtrata in base alla probabilità di essere SPAM. Delle analisi automatizzate definiscono il livello di "reputazione" dei messaggi basandosi su diversi elementi; se il livello di "reputazione" non è adeguato il messaggio viene considerato SPAM e inserito nella cartella "Posta indesiderata" invece che in "Posta in arrivo" all'interno della casella di posta dell'utente.

I messaggi di posta elettronica e dei programmi di collaborazione messi a disposizione dall'Ateneo subiscono la riscrittura dei link web contenuti al loro interno. In questo modo, se l'utente clicca su un link che è stato categorizzato come malevolo gli viene bloccato l'accesso alla risorsa web pericolosa.

Analogamente, i documenti allegati ai messaggi di posta, o condivisi attraverso programmi di collaborazione, vengono analizzati prima di essere resi disponibili all'utente oppure dopo che sono stati resi disponibili (purché si trovino nello spazio disco in cloud). Se i documenti sono ritenuti malevoli vengono cancellati o comunque resi inaccessibili all'utente.

È bloccato l'inoltro della posta elettronica di Ateneo verso caselle personali (non UNIPR), in quanto i messaggi inoltrati verso altri gestori di posta non vengono sottoposti ai controlli di sicurezza informatica predisposti dall'Ateneo (il blocco dell'inoltro è attivo dal 30 ottobre 2022 a seguito della "Nota del Rettore sulla sicurezza della posta elettronica" inviata al personale strutturato dell'Ateneo il 26 ottobre 2022).

4. Filtri sui flussi di dati delle reti interne

Il traffico dati che entra ed esce dalla rete interna dell'Ateneo viene filtrato per impedire l'accesso a risorse che possono veicolare Malware (es.: Ransomware, Botnet, DarkWeb, VPN anonime, SPAM URL, etc.), materiali illegali o inappropriati (es.: sostanze illecite, pornografia, estremismo, abusi, etc.), materiali coperti dal diritto d'autore. Il traffico viene filtrato sulla base di categorie predefinite e database di risorse notoriamente malevole.

I filtri vengono applicati per il traffico proveniente sia dall'infrastruttura di rete fisica (cablata) che dall'infrastruttura di rete wireless (WiFi).

Di seguito la tabella delle categorie dei contenuti filtrati e le relative azioni perimetrali.

Categorie	Azioni
Adult/mature Content	
Abortion	Allow
Advocacy Organizations	Allow

Alcohol	Allow
Alternative Beliefs	Allow
Dating	Allow
Gambling	Allow
Lingerie and Swimsuit	Allow
Marijuana	Allow
Nudity and Risque	Allow
Other Adult Materials	Allow
Pornography	Block
Sex Education	Allow
Sports Hunting and War Games	Allow
Tobacco	Allow
Weapons (Sales)	Allow
Bandwidth Consuming	
File Sharing and Storage	Allow
Freeware and Software Downloads	Allow
Internet Radio and TV	Allow
Internet Telephony	Allow
Peer-to-peer File Sharing	Block
Streaming Media and Download	Allow
Potentially Liable	
Child Abuse	Block
Discrimination	Allow
Drug Abuse	Allow
Explicit Violence	Block
Extremist Groups	Block
Hacking	Allow
Illegal or Unethical	Allow
Plagiarism	Allow
Proxy Avoidance	Block
Security Risk	
Dynamic DNS	Block
Malicious Websites	Block
Newly Observed Domain	Warning
Newly Registered Domain	Warning
Phishing	Block
Spam URLs	Block
Unrated	Warning

Allow: azione permessa

Block: azione negata

Warning: l'utente viene avvisato, ma può decidere di proseguire

Revisioni del documento

Ver.	Descrizione modifiche	Autore	Data modifica
1.0	*Versione iniziale*	*U.O. Sistemi Tecnologici e Infrastrutture*	*01/09/2021*
1.1	*Aggiunto blocco inoltro posta*	*U.O. Sicurezza IT*	*25/01/2023*
2.0	*Divisione filtri tra cloud e reti interne*	*U.O. Sicurezza IT*	*25/08/2023*