PHANTOM s.r.l

IMPOSSIBLE IS OUR TARGET

EPICODE

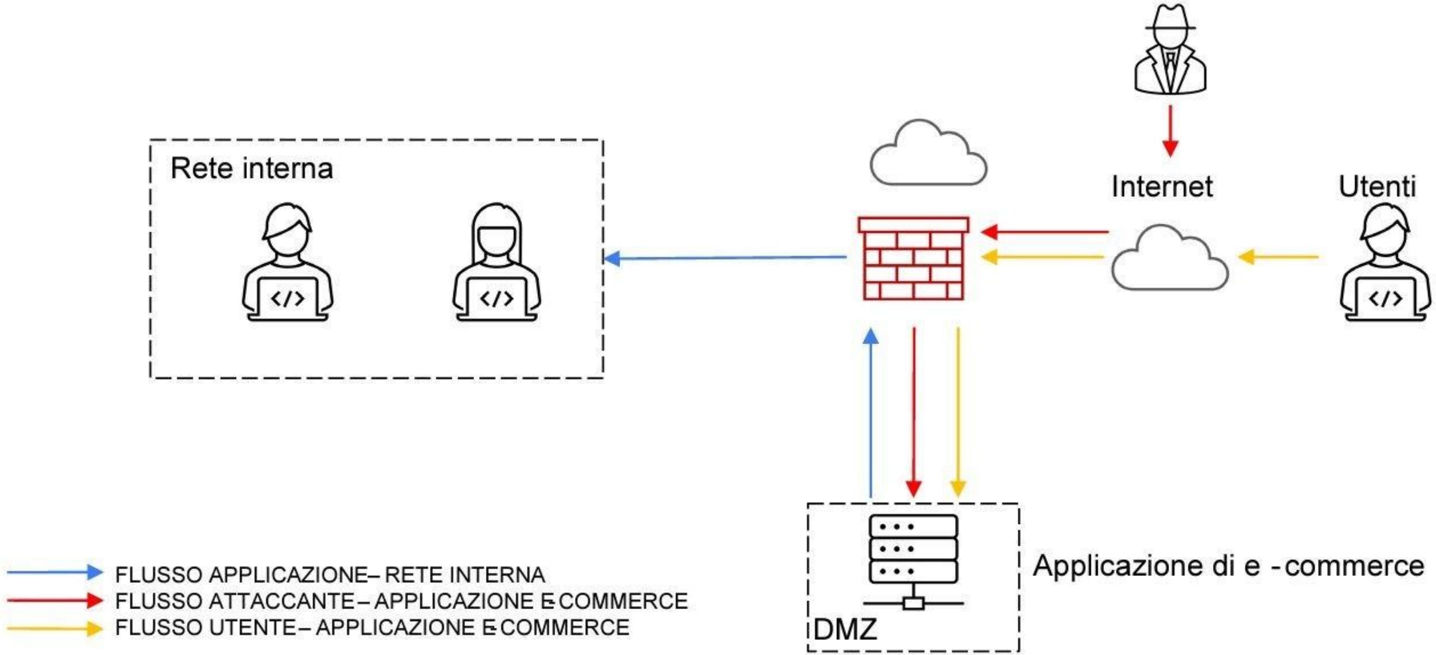
REPORT S9L5

PIO srl

Protecting is better than being safe

Defend the network

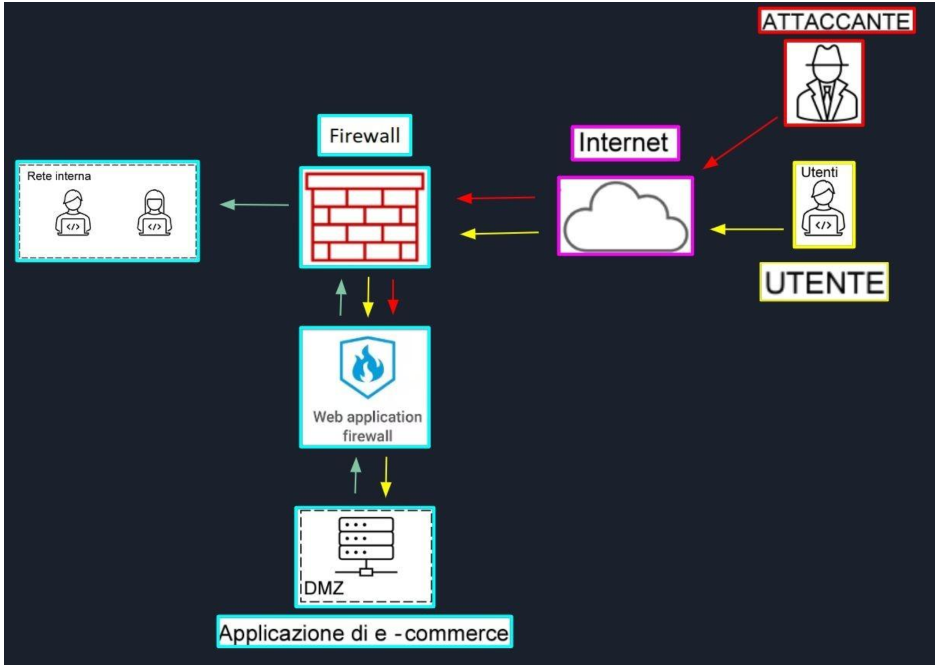
NETWORK ARCHITECTURE



FLUSSO APPLICAZIONE– RETE INTERNA
FLUSSO ATTACCANTE – APPLICAZIONE E COMMERCE
FLUSSO UTENTE – APPLICAZIONE E COMMERCE

SQLi and XSS Attack Prevention

In order to mitigate risks from *SQLi* (*SQL Injection*) and XSS (*Cross-Site Scripting*) attacks, which could threaten the security of our system, we have implemented a WAF (*Web Application Firewall)* to protect our web server. We are currently evaluating additional preventive measures, including sanitization of user input and continuous monitoring of network traffic, in order to further strengthen the security of our systems. Also, I kindly ask you to attach the new scheme with the implemented WAF.



EPICODE

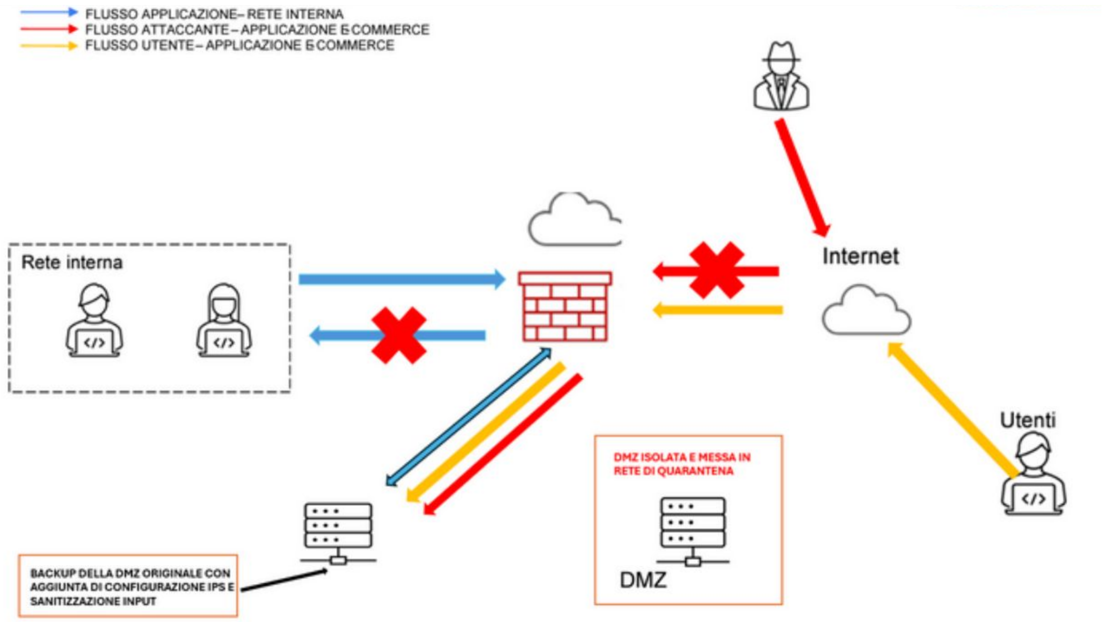
PHANTOM s.r.l
IMPOSSIBLE IS OUR TARGET

PIO srl
Protecting is better than being safe

"AGGRESSIVE" CHANGES

To further strengthen the security of the web application architecture
e-commerce, we have introduced an Intrusion Prevention System (IPS) directly into the Web Server. This IPS constantly monitors incoming and outgoing traffic to and from the server, identifying and blocking any attempted intrusions or cyber attacks. The presence of an IPS at the Web Server level adds an additional layer of protection against threats such as SQL Injection (SQLi), Cross-Site Scripting (XSS), and other application-level attacks.

In addition, to improve network management and better isolate different system components, we have divided the infrastructure into subnets. This division allows us to more efficiently organize network traffic and limit the potential attack surface, thereby increasing the resilience of the system to external threats. For example, we assigned a separate subnet for the Web Server and another subnet for the other infrastructure components, allowing more granular control over data flow and better management of security policies.


FLUSSO APPLICAZIONE– RETE INTERNA
FLUSSO ATTACCANTE – APPLICAZIONE E-COMMERCE
FLUSSO UTENTE – APPLICAZIONE E-COMMERCE
Rete interna
</>
</>
Internet
Utenti
</>
DMZ ISOLATA E MESSA IN RETE DI QUARANTENA
DMZ
BACKUP DELLA DMZ ORIGINALE CON AGGIIUNTA DI CONFIGURAZIONE IPS E SANITIZZAZIONE INPUT

EPICODE

PHANTOM s.r.l
IMPOSSIBLE IS OUR TARGET

PIO srl
Protecting is better than being safe

DDOS IMPACT AND PREVENTION

In the case of a hypothetical Distributed Denial of Service (DDoS) attack, it is assumed that the service becomes unreachable to customers for about 10 minutes. Users spend on average about 1,500€ every minute, on the platform. With a simple calculation, we can estimate a loss of about 15,000€ for a 10-minute outage. This loss could be reduced or avoided with a proper BCP (Business Continuity Plan), which would allow a service to continue operating even in critical situations, such as a DDoS attack, accidental damage or even natural disasters.

A viable BCP would be based on identifying and planning for risk factors, starting with the most critical and important ones (Risk Assessment), assessing the impact these would have on the business (BIA, Business Impact Analysis), training staff properly in order to implement the plan as efficiently and quickly as possible (to keep the service up and running to the best of ability), having backups available (can be secondary facilities, IT infrastructure replacements, and so on), and finally constantly improving and adapting it to cope with constant changes, both inside, and outside the company.

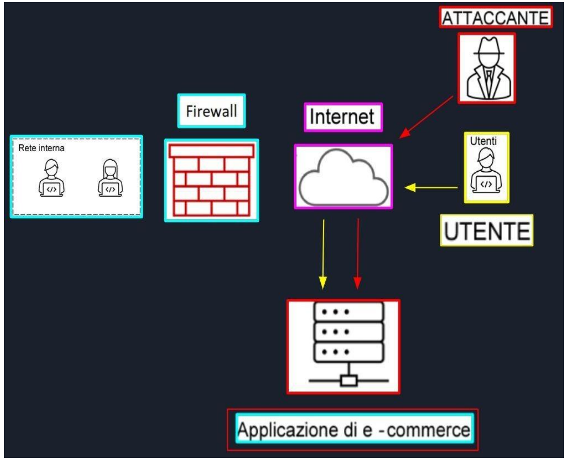
EPICODE

PHANTOM s.r.l
IMPOSSIBLE IS
OUR TARGET

PIO srl
Protecting is better than being safe

MALWARE RESPONSE

To design the company's internal network integration, we opted for isolation as the main strategy. This approach separates the web application from the rest of the enterprise, limiting the risk of spreading malware throughout the entire network. It is important to note that despite the isolation, an attacker with access to the web application of e-commerce could continue to have access, posing a possible security threat.

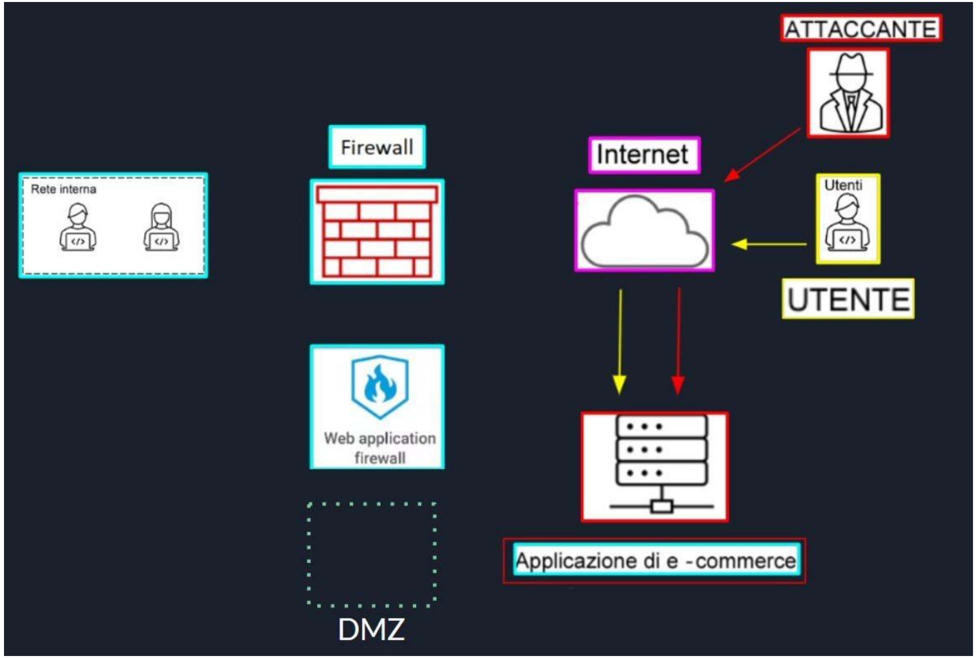


EPICODE

PHANTOM s.r.l
IMPOSSIBLE IS OUR TARGET

PIO srl
Protecting is better than being safe

COMPLETE SOLUTION



EPICODE

PHANTOM s.r.l
IMPOSSIBLE IS OUR TARGET

PIO srl
Protecting is better than being safe