

## Background Article

### Convergence with Web Application Security

## **The intelligent combination of protection mechanisms is critical for security**

**Attacks on web applications today are by no means coincidental, but deliberately targeted. As a result, the comprehensive and constant protection of web applications and services is both imperative and more important than ever before. Only a perfected solution that combines various security measures can identify and prevent even hitherto unknown attack methods early on and thus guarantee sustainable protection.**

In many companies, web application security measures are often still handled too separately from each other – either for historical or vendor-related reasons. This makes the security both unnecessarily complex and much less efficient. In order to be able to make the right security decisions at the applications level, different information must be available at the right time and in the right place. This is made much more difficult with selective, often uncoordinated activities in individual sub-areas. As a result, opportunities are opened up for attackers. In the case of Web Application Firewalls this applies in particular to authentication, access control, SSL termination, filtering, protocol validation and monitoring.

### **The main question is: who and what?**

Similar to with physical security measures at an airport, where tickets, passport, luggage and passengers are checked before boarding an airplane it is crucial that web applications security answers these questions in advance – that is: who someone is and what they are doing. The focus should be placed on this preceding authentication for web applications or environments with registered users. However, for publically accessible web applications and sites the most important aspect is filtering the protocols, requests and data. Since current web

applications usually include both, there is a demand for technical solutions which cover both issues efficiently and comprehensively.

The simplest example is applications with registered users who have to be authenticated, as is normal practice for example with e-banking or portals run by insurance companies, authorities or suppliers. The login page is publically accessible and is, as a result, open to attacks from all sides. This means that strict filter criteria are of critical importance in order to protect the login page. For the rest of the application it is however much more important that only correctly authenticated users are granted any access at all. These two issues can be combined perfectly with preceding authentication and comprehensive filtering in a Web Application Firewall (WAF).

### **Preceding authentication as an integral component in security concept**

In most companies the decision concerning the type of authentication is usually based on business and operational considerations. In addition mid-sized and larger enterprises often have more than one type of authentication in place – for example strong authentication for external access, a medium level for internal access or a separate variation for the B2B channel.

A Web Application Firewall such as phion Airlock offers the opportunity to enforce preceding authentication (Authentication Enforcement) and to delegate the check itself to the respective authentication service. This all happens completely independently of the specific type of authentication technology that is in place. A wide range of authentication alternatives and user directories can be addressed flexibly at the same time, even customer-specific IAMs (Identity Access Management).

A company can realise two significant advantages with the preceding authentication method: Firstly, the applications are completely protected against anonymous access (this applies for all levels such as TCP/IP, SSL, HTTP, application servers, operating system, libraries; business logic and others too).

This then greatly reduces the threats and risk of attack for the authenticated applications. Secondly, the one-off connection between the authentication and the WAF is much more efficient and flexible. The company can decide about the type of authentication without having to adapt all applications at any time. If required, a Single Sign On with a PKI solution can be implemented without the protected applications having to know anything at all about the PKI solution. This advantage not only saves the company money and increases flexibility because new applications can be integrated much more simply into the environment, but also improves the security in a sustained manner.

### **Simultaneous monitoring benefits from combined approach**

A central WAF, which takes care of both the authentication and the constant filtering of all requests and data as a secured Reverse Proxy, offers the company all relevant information about WHO has done WHAT in the entire web environment at any time. As such, the sender of an activating request is immediately visible in a triggered White List Filter within an e-banking session – as are his activities during the application session.

Armed with this information, which is only available in a combined approach between preceding authentication, comprehensive filtering, SSL termination, secure session handling and other functions in this quality, those responsible for security win time and can act proactively.

### **A brief description of preceding authentication**

Preceding authentication prevents web servers from being exposed to anonymous connections. In this way the number of potential attackers can be massively reduced and the applications are relieved. In addition the preceding authentication also facilitates centralised access control which is distinct from the business logic. This increases the security and at the same time reduces the costs. Only authenticated and authorised connections are granted access to the respective applications servers.



### **About phion**

phion is one of the leading European providers of solutions to protect company communications. With the netfence product portfolio phion offers solutions for the most demanding standards in terms of availability, security and management. netfence appliances consistently address all security-related aspects: From perimeter defence to the safe and highly available connections to branch offices, right up to blocking dangerous contents and protecting internal networks. airlock protects web applications like e-banking platforms and web services from any attacks or misuse.

All phion products have core management and are distinguished by their remarkable TCO.

phion is listed at the Vienna stock exchange (symbol: PHIO) and is based in Innsbruck, Austria and Zurich, Switzerland. phion's customers include well-known, internationally operating companies from all sectors of industry.