Sichere Digitalisierung mit vorgelagertem Schutz und flexibler Authentisierung

Marc Bütikofer, Director Innovation Airlock

Ergon Informatik AG

Kompetent in IT Security: Airlock Suite bringt mehr…

Expertenwissen seit 15 Jahren

Wir schützen mehrere tausend Anwendungen und Millionen Benutzer

Mehr als 350 Kunden mit mehreren 1000 Instanzen

50 Ingenieure sorgen im Airlock Team für Sicherheit

150 Banken und Versicherungen vertrauen auf Airlock

11 Millionen Umsatz in 2015

Business Partner hp invent

PCI SECURITY VENDOR ALLIANCE

OWASP Open Web Application Security Project

SWISS TECHNOLOGY AWARD

EBA EUROPEAN BANKING AUTHORITY

eicar trusted IT-security

Teilnehmer der Allianz für Cyber-Sicherheit

MAS Monetary Authority of Singapore

PC Magazin

Tests | Kaufberatung | Ratgeber | News | Business & IT | Downl

Home » News » Sicherheit » Kaspersky Internet Security weiterhin durch FREAK verwundbar

Empfehlen 2 | Twittern 3 | +1 0 | Weitersagen | Drucken

FREAK-Sicherheitslücke 28.04.2015

Kaspersky Internet Security weiterhin durch FREAK verwundbar

In einem Test stellte sich heraus, dass die Antiviren-Software Kaspersky Internet Security weiterhin über die SSL-Sicherheitslücke FREAK verwundbar ist.

Google-Anzeigen

(Neu) Wingo

Einfach, Transparent, Ehrlich. What you see is what you get! www.wingo.ch

AP systems remain unpatched attacks

Onapsis found that most SAP systems remain vulnerable to attacks that could compromise a company's business data and processes.

exposed to
r to fully
and
m SAP

for years,
interview
g somewhat

erstood,
91 security
. Nearly 50 percent of those patches were considered "high priority,

HEARTBLEED, SHELLSHOCK UND CO

Warum das In muss

Christof Kerkmann
13.10.2014 06:45 Uhr

artbleed, dann Shel
heitslücken haben di
eren ein gravierende
Software - aber nur

SICHERHEITSLÜCKE HEARTBLEED

Der Schock wirkt noch nach

Autor: Christof Kerkmann
Datum: 10.10.2014 13:00 Uhr • 10.10.2014, 16:00 Uhr

Heartbleed ist nicht mehr in den Schlagzeilen - und trotzdem noch ein Problem. Viele Webseiten sind noch immer nicht gegen die Schwachstelle in der Verschlüsselungssoftware OpenSSL abgesichert. Eine Zwischenbilanz.

Heartbleed: Ein halbes Jahr nach der Entdeckung

COMPUTERWOCHE

MEET THE IBM EXPERTS

Security

Cybercrime

Swift warnt vor Angriffswelle auf Banken

13.05.2016

Internationale Finanzströme geraten verstärkt ins Visier von Cyberkriminellen. Nach einem 80-Millionen-Coup wurde jetzt schon die zweite Attacke auf eine Bank innerhalb weniger Monate bekannt. Die EZB will nun eine Meldestelle einrichten.

Empfehlen
Diskutieren
Drucken
PDF
URL
Xing
LinkedIn
Twitter
Google+
Facebook

Nach dem spektakulären 80-Millionen-Dollar-Raub bei der Zentralbank von Bangladesh haben Cyberkriminelle erneut ein Zahlungsinstitut ins Visier genommen. Offenbar handele es sich um einen Teil einer größer angelegten und sehr anpassungsfähigen Kampagne, warnte das internationale Zahlungsverkehrssystem Swift am Freitag. In beiden Fällen seien die Angreifer in ähnlicher Weise vorgegangen. Um welche Bank es sich dabei handelt und ob bereits Schaden entstanden ist, teilte die Organisation nicht mit.

Im Februar hatte eine Attacke auf die Zentralbank in Bangladesh für internationales Aufsehen gesorgt. Den Angreifern gelang es, 81 Millionen Dollar zu erbeuten. Zuvor knackten sie das Sicherheitssystem der Bank. Vermutlich hatten die Cyberkriminellen es auf eine noch viel höhere Summe abgesehen, flogen jedoch vorher auf. Im März spürte Swift eine betrügerische Software auf, mit der Angreifer gezielt Geldströme zu verschleiern suchten.

Shellshock sorgt für Open Source Debatten - computerworld.ch

26. Sept. 2014 ... Einen Ta
wieder Nüchternheit ... Hac
www.computerworld.ch/.../

DDoS-Angriff

8. Mai 2015 ... Ein
lahm. Besonders
www.computerwo

SPIEGEL ONLINE NETZWELT

Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | Gesundheit | einestages | Karriere | Uni

Nachrichten > Netzwelt > Web > Computersicherheit > Hacker-Angriff auf polnische Airline LOT in Warschau

Flüge gestrichen: Hacker-Angriff auf polnische Airline L

DPA

Lot-Flugzeug in Warschau (Archivbild): "Dieser Vorfall könnte auch anderen drohen"

Gestrichene Flüge und gestrandete Passagiere: Ein Hacker-Angriff hat das Computersystem der staatlichen polnischen Airline am Flughafen von Warschau lahmgelegt. Fünf Stunden lang ging bei LOT nichts.

Handel

AUF „HE

«Venom»-Sicherheit

vor 6 Tagen ... Heartblee
dementsprechend kann e
www.computerworld.ch/...
en-67921/

Autor:
Datum: 15.10.2014 16:30 Uhr

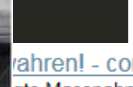
Die SSL-Verschlüsselung
Experten spätestens seit
haben Google-Experten ei
entdeckt.

Sicherh

6. März 2
betroffen,
durchzufü
www.com
Label Bus

Die betroffene Version der SSL-Verschlüsselung ist rund 15 Jahre alt, aber die aktuell
Browser unterstützen sie noch. (Foto: Reuters)

ver UPDATE



wahren! - computerworld.ch

gte Massnahmen gegen die OpenSSL-Lücke
APT-**Angriffe** (Advanced Persistent Threats)

s/.../**heartbleed**-ruhe-bewahren-65593/

eded)

om" bezeichnet - was einerseits Gift heißt und die
rakterisiert, andererseits auch als Kürzel für "Virtualized
ns Manipulation" dient. Das deutet bereits darauf hin, dass
Virtualisierungs-Umgebungen zu tun haben.

urde, ist zurück
n hier über
ausführen.

er Fehler durch den Sicherheitsforscher Jason Geffner, der
tellt ist. Dieser kommt zu dem Schluss, dass Venom
bleed ist. Bei letzterem handelte es sich um einen Bug im
glichte es einem Angreifer, die in den verschlüsselten
mationen auszulesen.

Motivation Hacker

Zero-Day-Schwachstellen -> mehrere 100.000 $

2015 laut Symantec 54 Zero-Day Schwachstellen

In Zahlen

429 Mio.
Identitäten wurden 2015 laut Symantec in 305 Fällen von Datendiebstahl entwendet.

78%
aller von Symantec 2015 gemessenen Websites wiesen Schwachstellen auf. Bei 15% waren es gar kritische Lücken.

1,1 Mio.
Bots gab es 2015. Dies sind befallene Computer, die von Cyberkriminellen für Attacken oder als Spamschleuder genutzt werden.

AIRLOCK

Virus zu verkaufen

Welche Daten und Dienste auf dem Marktplatz der Hacker angeboten werden

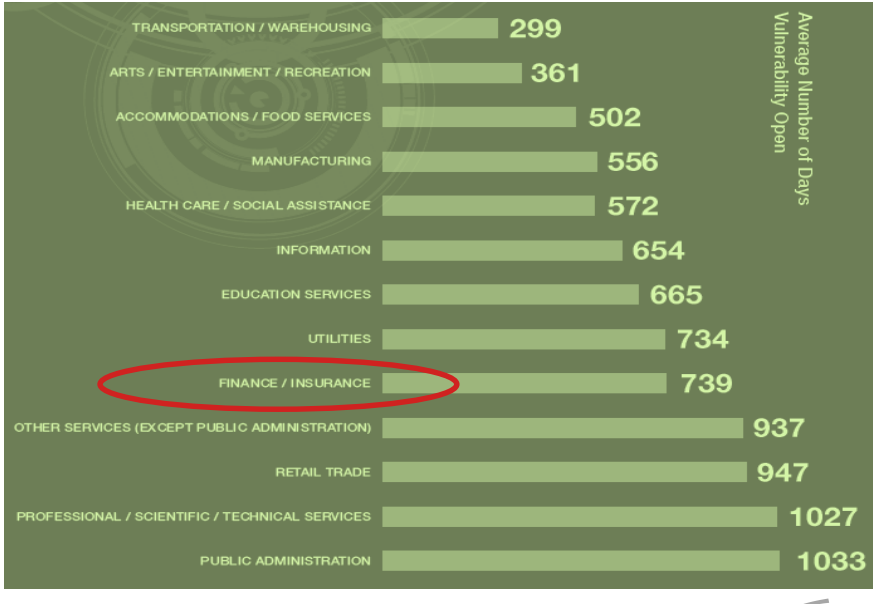
Kreditkartendaten	Preise 2014	Preise 2015
Visa und Mastercard (USA)	4 $	7 $
Visa Classic und Mastercard Standard (EU)[1]	28 $	40 $
Identitäts-Diebstahl		
E-Mail-Konto (Gmail, Hotmail, Yahoo)	–	129 $
Social-Media-Accounts (Facebook, Twitter)	–	129 $
Firmen-E-Mail-Konto	–	500 $
Vollständiges Identitäts-Dossier (USA)	30 $	15–65 $
Gefälschter physischer US-Pass	–	3000–10000 $
Vorlage für US-Pass	–	100–300 $
Gefälschter physischer Fahrausweis (Frankreich)	–	238 $
Zugriff auf Online-Bezahldienste wie Paypal		
Übertragung von Geld auf Konto der Wahl		25–30%[2]
Zugangsinformationen		24–63%[2]
Zugriff auf Bankkonten		
Britisches Bankkonto (Kontostand: 27000 $)		2000 $
US-Bankkonto (Kontostand: 15000 $)		500 $
Bankkonto mit verifiziertem Kontostand von 70000 bis 150000 $		6%[2]
1,5 Millionen Frequent-Flyer-Meilen einer US-Fluggesellschaft		450 $
1 Million Punkte einer grossen internationalen Hotelkette		200 $
Hacker-Werkzeuge		
Trojaner für Fernzugriff	20–50 $	5–10 $
Viren-Tarnprogramme (Crypters)	50–150 $	80–440 $
Angler-Exploit-Kit (beliebtes, effektives Angriffswerkzeug)	–	100–135 $
Hacking-Dienstleistungen		
Mehrere Schnellkurse	30 $	20–40 $
DDoS-Attacken pro Stunde	3–5 $	5–10 $
DDoS-Attacken pro Tag	60–90 $	30–55 $
DDoS-Attacken pro Woche	350–600 $	200–555 $

[1] Mit Magnetstreifeninformationen [2] Prozent des Kontostandes

Quelle: SecureWorks

Bedrohungen

Quelle Whitehat Web Security Report 2015



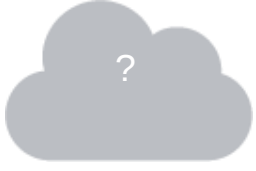
Airlock Suite

Web Application Firewall & Identity and Access Management

Was wird für eine hohe Applikationssicherheit benötigt

Mit wem haben wir es zu tun?

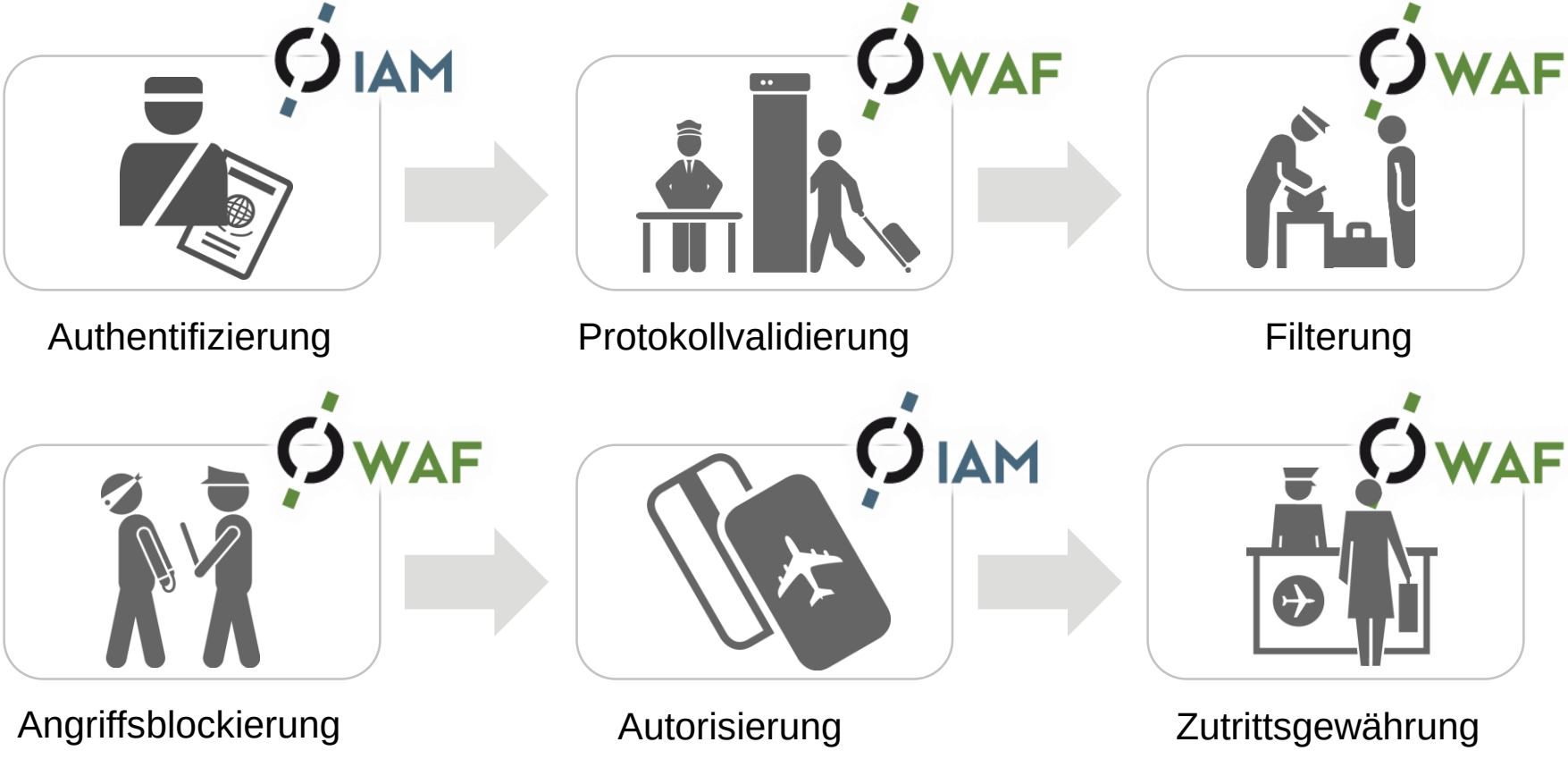
Zugriffs-
kontrolle → IAM



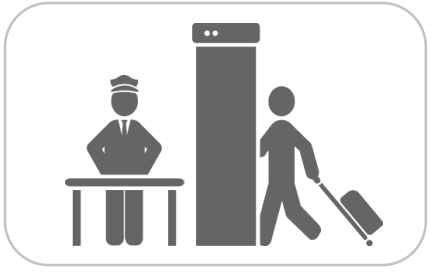
Womit haben wir es zu tun?

Filter → WAF

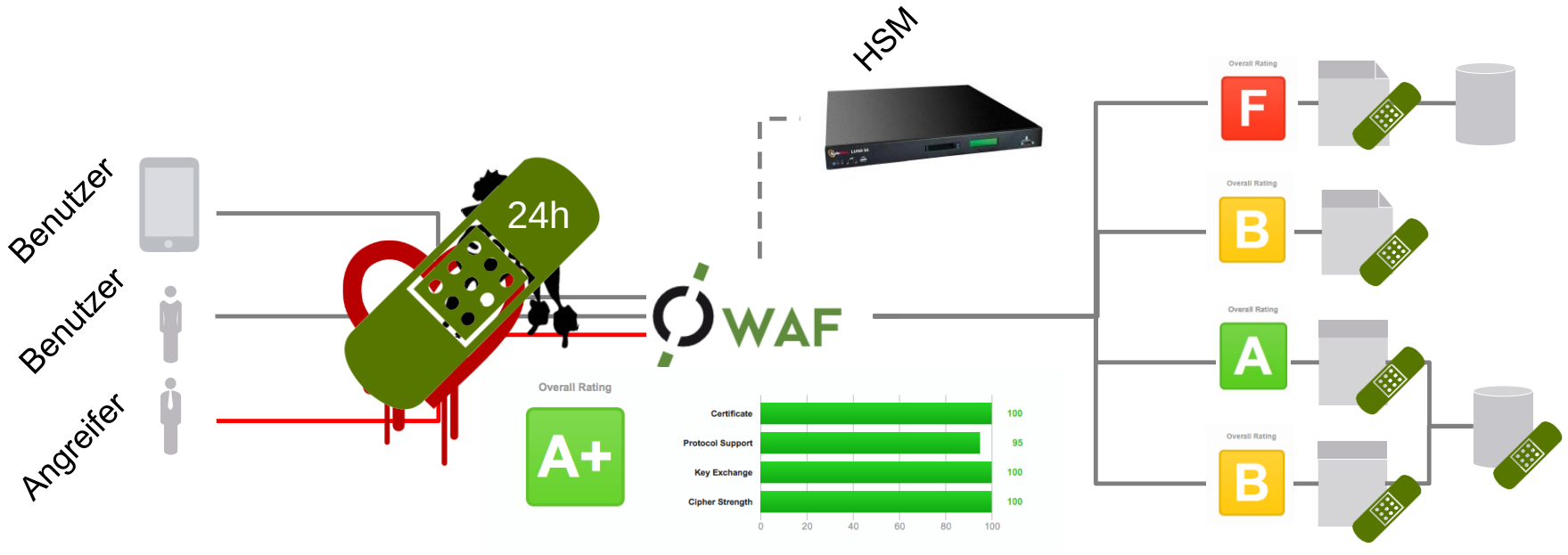
Vorgelagerte Sicherheit



Airlock WAF - Mehrstufige Filter



Schnelle Reaktionsmöglichkeit auf neue Angriffsvektoren



Hauptkriterien für Applikationssicherheit

Mit wem haben wir es zu tun? Zugriffskontrolle

Vielzahl von Authentisierungsmöglichkeiten

Benutzerberechtigungsverfahren

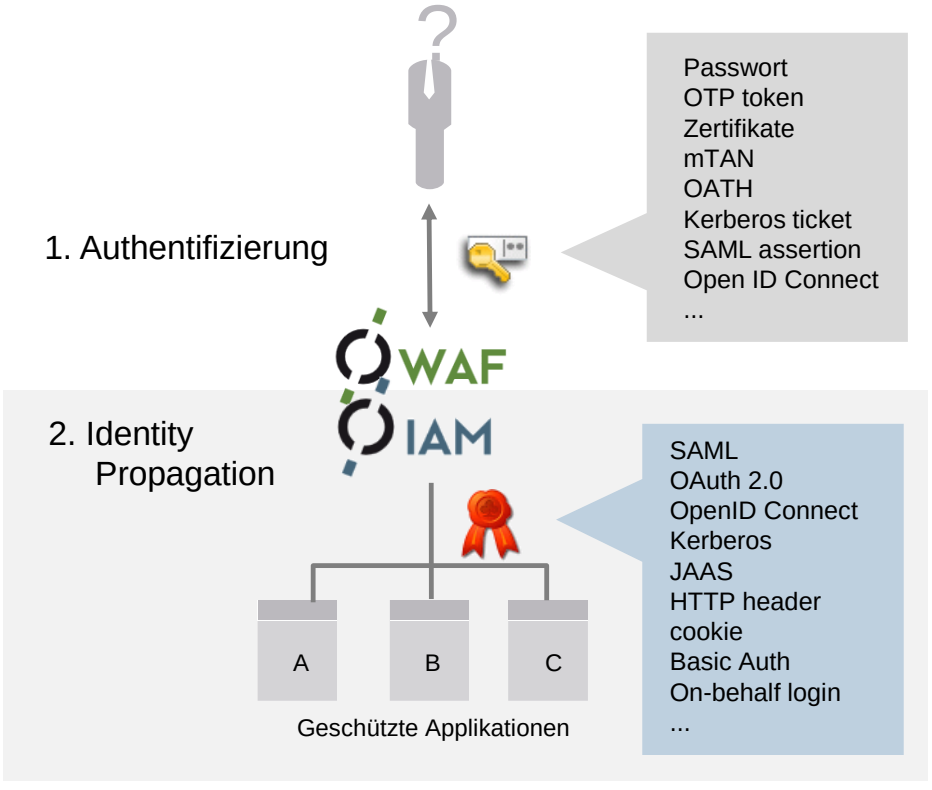
Zugriff auf Applikation erfordert

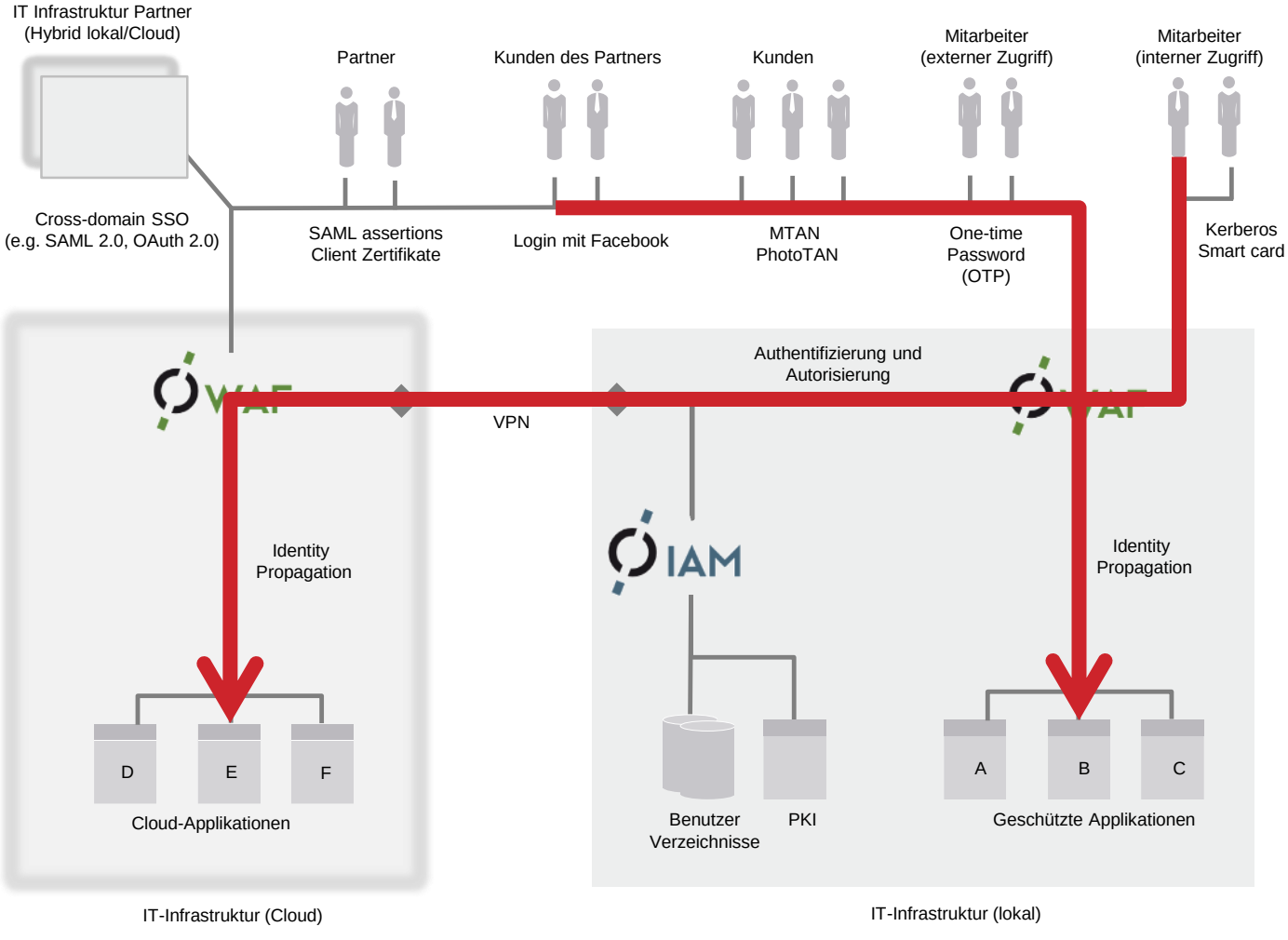
1. Authentifizierte Benutzeridentität
2. Autorisierung des Zugriffs

Berechtigung (Autorisierung) basiert auf

– Zielapplikation
– Gruppenzugehörigkeit
– Benutzerattribute
– Authentifizierungsstärke (z.B. Step-up Authentifizierung)
– Kontext der Session (IP Adresse, Browser Fingerprint, Tageszeit, etc.)

Trennung von Authentifizierung und Identity Propagation




IT Infrastruktur Partner
(Hybrid lokal/Cloud)
Partner
Kunden des Partners
Kunden
Mitarbeiter
(externer Zugriff)
Mitarbeiter
(interner Zugriff)
Cross-domain SSO
(e.g. SAML 2.0, OAuth 2.0)
SAML assertions
Client Zertifikate
Login mit Facebook
MTAN
PhotoTAN
One-time
Password
(OTP)
Kerberos
Smart card
WAF
Authentifizierung und
Autorisierung
WAF
VPN
Identity
Propagation
IAM
Identity
Propagation
D
E
F
Cloud-Applikationen
Benutzer
Verzeichnisse
PKI
A
B
C
Geschützte Applikationen
IT-Infrastruktur (Cloud)
IT-Infrastruktur (lokal)

Zusammenfassung

Web Applikationen sind hohen Risiken ausgesetzt

Schutz vorgelagert und spezialisiert.

Vielfach bewährte Architektur.

Filterung von Web Requests.

Schnelle Reaktion auf neue Risiken

Hohe Flexibilität in Authentisierung.

Trennung Authentisierung und ID-Propagation

15 Jahre Erfahrung
Viele Referenzen

Swiss made Security