Případová studie nasazení F5 v SITMP

Zabezpečený přístup k aplikacím & WAF

PRESENTED BY:

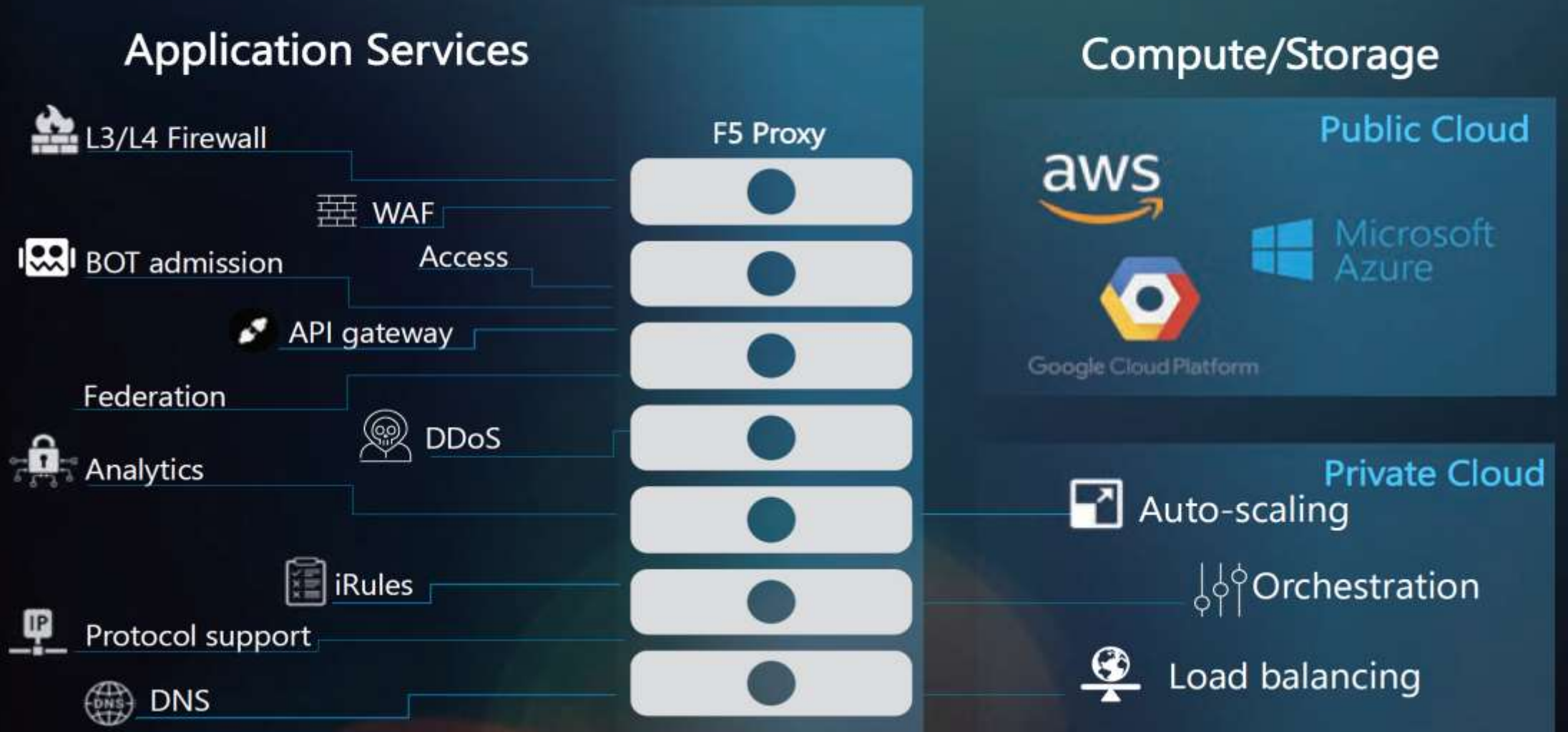
Martin Kylián - Network Security Engineer, Správa informačních technologií města Plzně

Filip Kolář – Account manager, Networks ČR

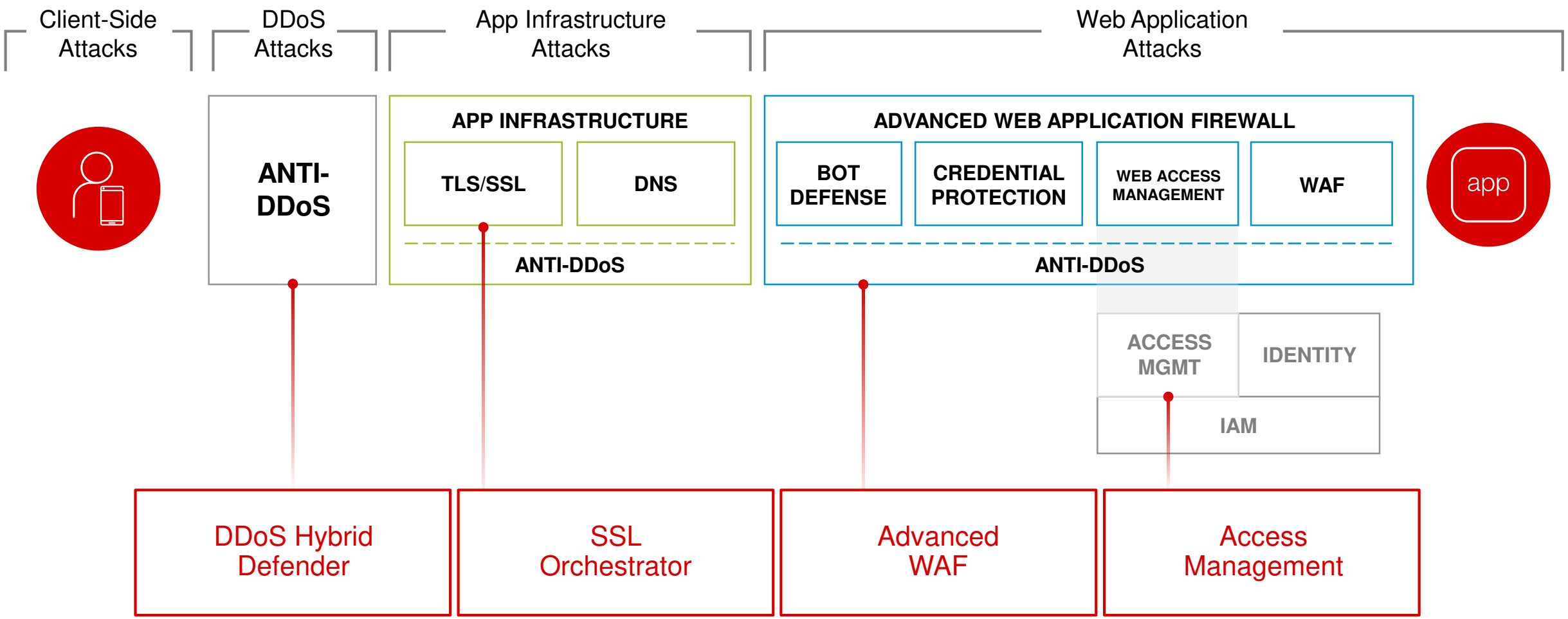
Radovan Gibala, Systémový inženýr, F5 Networks ČR

WE MAKE APPS GO FASTER. SMARTER. SAFER.

F5 portfolio introduction



Complete App Protection Framework



Správa informačních technologií Plzeň

Případová studie nasazení F5 v SITMP

Load Balancing, WAF, IAM

ISSS, ing. Martin Kylián

1. dubna 2019

Kdo je to SITMP

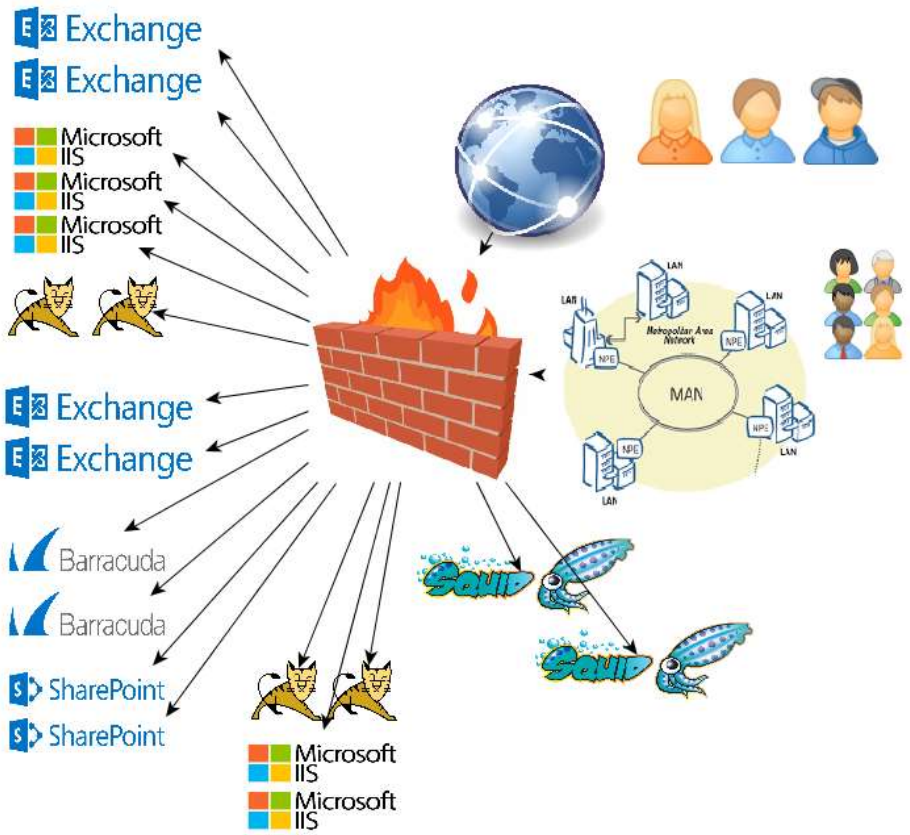
- IT pro ~100 organizací v Plzni
- 20.000 uživatelských identit
- Úřady
- Školy
- Sportovní areály…

Co zajišťujeme

- Výpočetní technika
- Metropolitní síť
- Datová centra
- Aplikace
- Procesy
- Kyberbezpečnost
- Vzdělávání

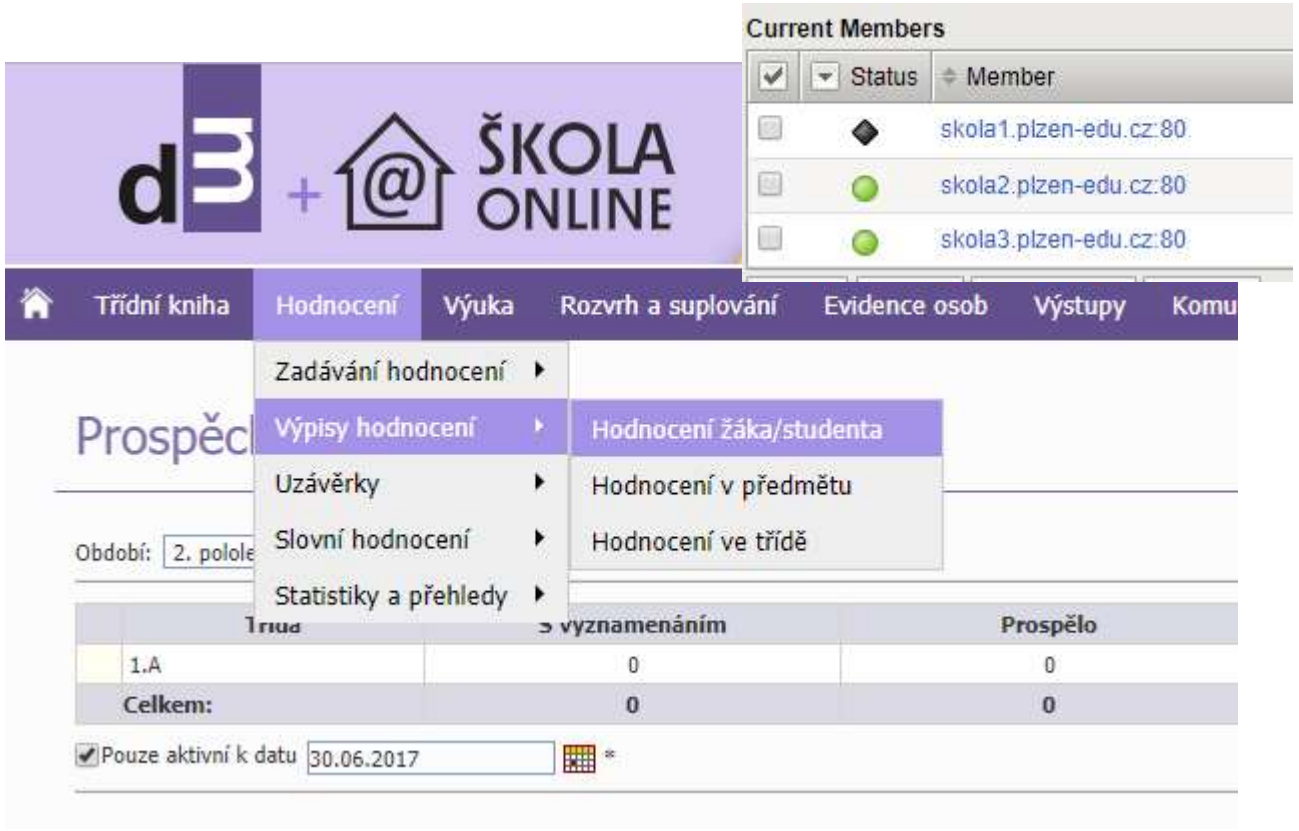
Kde jsme byli

- Několik Core služeb
- MS Exchange, MS Sharepoint
- Různé: webové servery a technologie, aplikace, správci



Cíl č.1 – vysoká dostupnost

- SMTP Gatewaye
- Exchange
- Škola on-line
- Http proxy



Sekundární přínosy LB

- Centrální správa SSL certifikátů
- Centrální správa celého SSL stacku / offload SSL

Na co si dát pozor

- Stavové aplikace – persistence Sessions
- Správné url – wsdl, odkazy na assety…

Cíl č.2 – bezpečnost web aplikací

Klíčové vlastnosti

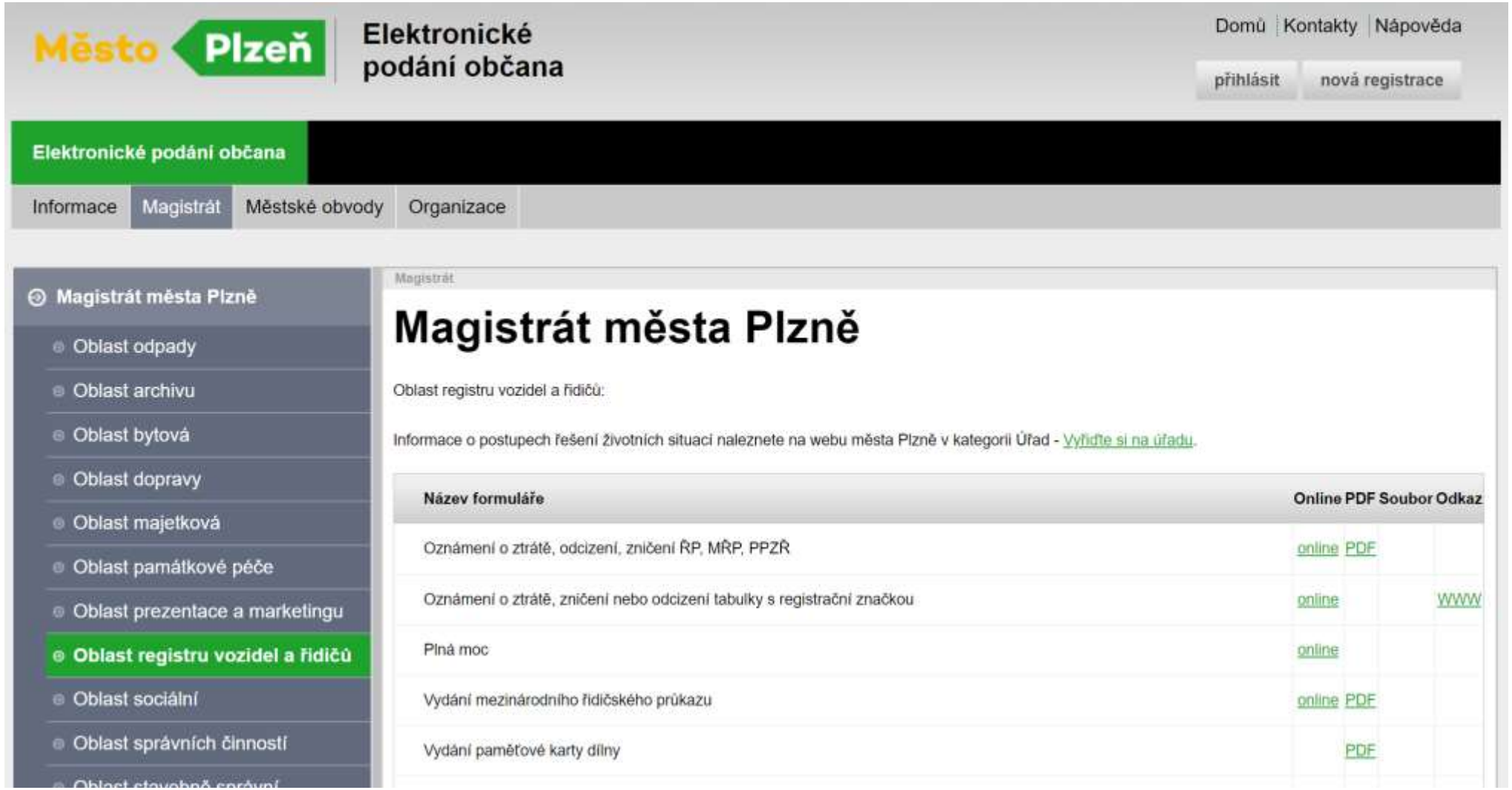
- OWASP top 10
- Ochrana přihlašovacích formulářů

Nejzranitelnější systémy

- Redakční systém bez podpory výrobce (~150 webů)
- Hostingové servery – WP, Joomla, Drupal

Portál občana

Portál občana



WAF - když to funguje

SQL Inj

```
Accept-Language: cs-CZ,cs;q=0.9
Cookie: f5_cspm=1234; JSESSIONID=62557EBE1635B95075D98B64CC718A97; TS0118f59c=0144410629c113220bfa8974b56eecb9853a4ffc57bb6b86ee4e61172ec6ea520aae777ed38a82e66302f035fff90810c9
c183c0cd95161e7046d962424e5947a641709d22; JSESSIONID=DFFC487E7408E2C0CCC4023A862F9C0C; tritius_sql_history=select * from user where id = 7||SELECT count(*) FROM table_column_co
nfig WHERE header_config_root = -1179 and name = 'workType' and hs_path like 'G3803'|SELECT count(*) FROM table_column_config WHERE header_config_root = -1179 and name = 'workT
ype'|SELECT * FROM table_column_config WHERE header_config_root = -1179 and name = 'workType'||select count(*) from user_to_user_group where user = 7|select * from user_to_user
_group where user = 7||select * from charge_history where reader = 60753||select * from charge_history where reader = 19676||select * from borrow_cycle where reader = 61394||;
 TS01b16c26=01444106292b83cbb09c32b07126700f6f8db7c00a0d5c68cc37905fcd80c426ac543747d2c929273cce4111dc23807ddb7e2bfe5b3da8acb09e4c05424bd568fce31d1a60461186bf421ada36c9d1e25ab1
ac759d
```

```
GET /irj/portal/anonymous?NavigationTarget=ROLES://portal_content/IUO/Role/IUO_Anonymni/Elektronick__pod_n__ob_ana_1/Elektronickpodnobana/ID_MESTSKE_OBVODY_PAGE&obvod=MO3&oblas
t=stav UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL# HTTP/1.0
```

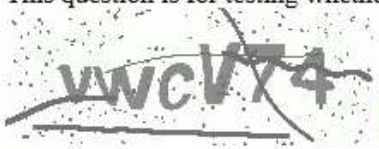
Logon form protection

Brute Force: Maximum login attempts are exceeded [1]

Mitigated Action	Alarm and Blocking Page
Username	Hhhhh
Detected Failed Logins / Threshold	4 / 3 (at the time of attack detection)
Detection Period	60 minutes
Maximum Prevention Duration	60 minutes
Applied Blocking Settings	Block Alarm

```
POST /_Admin/LogIN/Default.aspx?ReturnUrl=/_Admin HTTP/1.1
```

This question is for testing whether you are a human visitor and to prevent automated spam submission.



What code is in the image?

submit

Your support ID is: 10419132438721077370.

WAF – na co dbát při nasazení

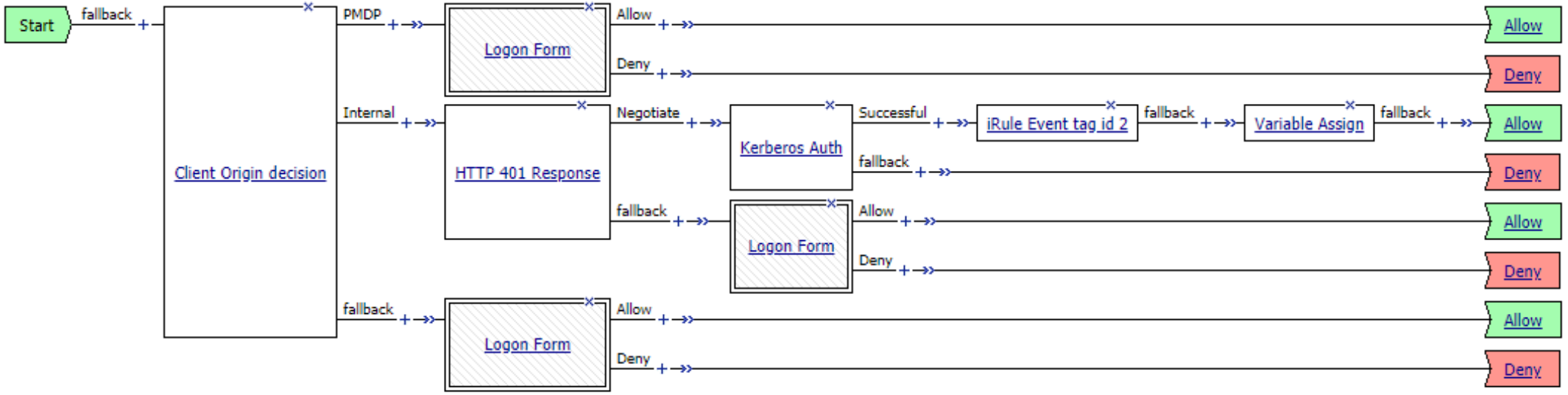
- Znalost aplikace nebo alespoň principů
- Cílit na přesné nastavení
- False pozitiva v negativním modelu / využívat staging
- Vše co nejlépe testovat

Cíl č.3 – identity access

Aplikace - chceme zpřístupnit, ale jen někomu

Naše další požadavky

- SSO
- Možnost řídit přístupové role
- Integrace s 2FA (připravujeme)



31383175	View	[redacted]@PLZEN-CITY.CZ	192.168.90.78	/Common/VS_[redacted]plzen.eu	2019-03-28 10:52:02	2019-03-28 16:42:05	3890519	33879456	ltm_apm
a26f9026	View	[redacted]@PLZEN-CITY.CZ	192.168.90.57	/Common/VS_[redacted]eu_HTTPS	2019-03-28 14:39:55	2019-03-28 15:10:30	1025024	1838486	ltm_apm
0a295465	View	[redacted]	2a07:8d80:800:f17a:94f5:f3f3:8e37:9d37	/Common/VS_[redacted]plzen.eu_v6	2019-03-28 13:14:08	2019-03-28 17:15:55	122126	3091494	ltm_apm
cbf215c4	View	[redacted]@PLZEN-CITY.CZ	192.168.13.45	/Common/VS_[redacted]plzen.eu	2019-03-28 14:12:36	2019-03-28 18:13:02	100314	805443	ltm_apm
faa29556	View	[redacted]@PLZEN-CITY.CZ	192.168.90.116	/Common/VS_[redacted]_HTTPS	2019-03-28 14:57:14	2019-03-28 15:27:35	225059	1049275	ltm_apm
598e1d1e	View	n/a	54.37.23.163	/Common/VS_[redacted]plzen.eu	2019-03-28 14:54:49	2019-03-28 14:59:49	0	0	n/a
3df3c3fc	View	n/a	192.168.248.44	/Common/VS_[redacted]_HTTPS	2019-03-28 14:57:40	2019-03-28 15:02:40	0	0	n/a
055a7933	View	n/a	54.37.22.123	/Common/VS_[redacted]plzen.eu	2019-03-28 14:53:10	2019-03-28 14:58:10	0	0	n/a

Obecné poznatky z nasazení

K nasazení f5 je potřeba

- Síťový specialista
- Aplikačního správce
- Bezpečnostního specialistu
- Programátora

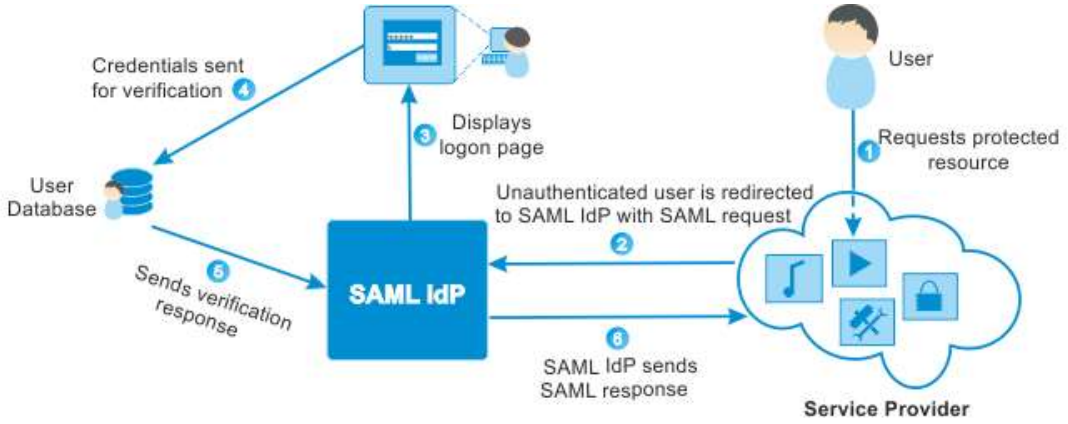
Shrnutí

Díky technologii f5 se nám podařilo

- Zajistit bezvýpadkový provoz
- Zabezpečit zranitelné aplikace
- Efektivně řídit přístupy k aplikacím

Kam dál?

- Saml IdP



Client-side Authentication Methods	Server-side Authentication Methods: HTTP Form	HTTP Basic	NTLM	Kerberos
HTTP Form	Yes	Yes	Yes	Yes
HTTP Basic	Yes	Yes	Yes	Yes
NTLM	No	No	No	Yes
Kerberos	No	No	No	Yes
Certificate	No	No	No	Yes
SAML[1]	Yes	Yes	Yes	Yes
RSA SecurID	No[2]	No[2]	No[2]	No[2]
One-Time Passcode	No[2]	No[2]	No[2]	No[2]

- Podpora kontejnerů

F5 Kubernetes BIG-IP Controller

F5 Kubernetes BIG-IP Controller manages F5 BIG-IP Local Traffic Manager (LTM) objects from Kubernetes.