DSGVO: Konkrete Hilfe bei der Umsetzung

Was bei der Verarbeitung von personenbezogenen Daten in Web-Anwendungen zu beachten ist

Agenda

Einführung DSGVO	Arne Arnold, freier Redakteur für COMPUTERWOCHE
Risikobewusstsein und -minimierung unter der DSGVO	Dr. Anna Schmits, EMEA Datenschutzbeauftragte, Akamai
Adaption und Prävention auf der technischen Ebene	Gerhard Giese, Manager Enterprise Security Architects EMEA, Akamai

©2017 AKAMAI

Akamai

Datenschutz-Grundverordnung

Risikobewusstsein und -minimierung unter der DSGVO

Dr. Anna Schmits
EMEA Datenschutzbeauftragte
Akamai Technologies

26. Oktober 2017

DSGVO

- Die EU **D**aten**s**chutz **G**rund**v**er**o**rdnung, ist das **neue EU Datenschutzgesetz**.
- Sie tritt am **25. Mai 2018** in Kraft.
- Sie regelt die **Verarbeitung personenbezogener Daten von EU Bürgern.**
- Sie gilt innerhalb und **außerhalb der EU.**

©2017 AKAMAI

Akamai

DSGVO – Risikobewusstsein und -minimierung

- **Ziele der DSGVO:**
  - Umfänglicher Schutz der EU Bürger.
  - Rechenschaftspflicht des datenverarbeitenden Unternehmens.
- **Rechte des Betroffenen:**
  - Recht auf Zugang zu den Daten.
  - Recht auf Richtigstellung.
  - Recht auf Löschung.
  - Recht auf Vergessen.
- **Die Rechenschaftspflicht** zielt darauf ab, das datenverarbeitende Unternehmen verantwortlich zu machen und die Einhaltung der DSGVO nachzuweisen zu lassen.

©2017 AKAMAI

Akamai

DSGVO – Risikobewusstsein und -minimierung

Die Datenschutz-Folgenabschätzung:

- **Abschätzung der Folgen der Verarbeitung,** für die Rechte und Freiheiten natürlicher Personen

- **Was für Risiken bestehen unter Beachtung:**
  - ✓ der Art der personenbezogenen Daten,
  - ✓ der jeweiligen Verarbeitungsvorgänge,
  - ✓ der getroffenen Maßnahmen zum Schutz der Daten?

©2017 AKAMAI

Akamai

DSGVO – Risikobewusstsein und -minimierung

- **Geeignete Maßnahmen** zum Schutz personenbezogener Daten.

- **Hinweise**, was angemessen ist:
  Verschlüsselung, Pseudonymisierung und Anonymisierung.

- **Weitere Beispiele** sind in dem ISO 27001 Standard und in dem Anhang zu § 9 des BDSG zu finden.

- Ziel ist es, das **Risiko zu minimieren**, dass mit der Datenverarbeitung verbunden ist.

©2017 AKAMAI

Akamai

Adaption und Prävention auf der technischen Ebene

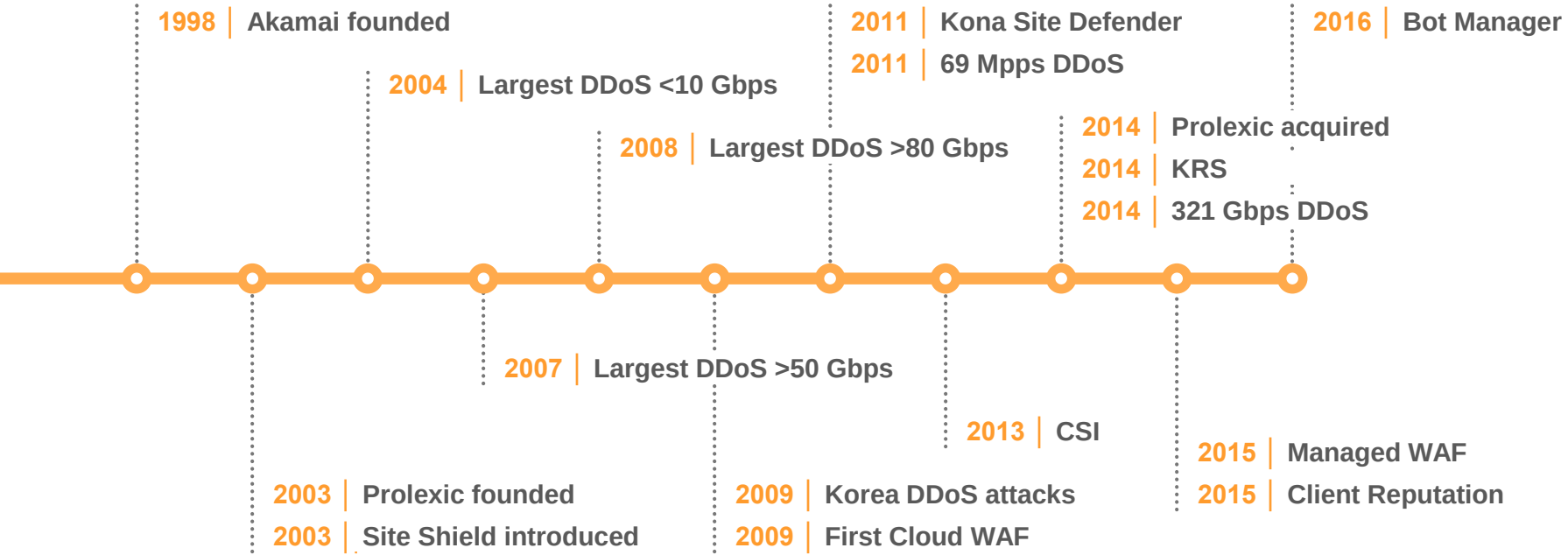
Wie Akamai bei der Einhaltung der DSGVO unterstützt

Gerhard Giese
Manager Enterprise Security Architects EMEA
Akamai Technologies

26. Oktober 2017

Security Know-how

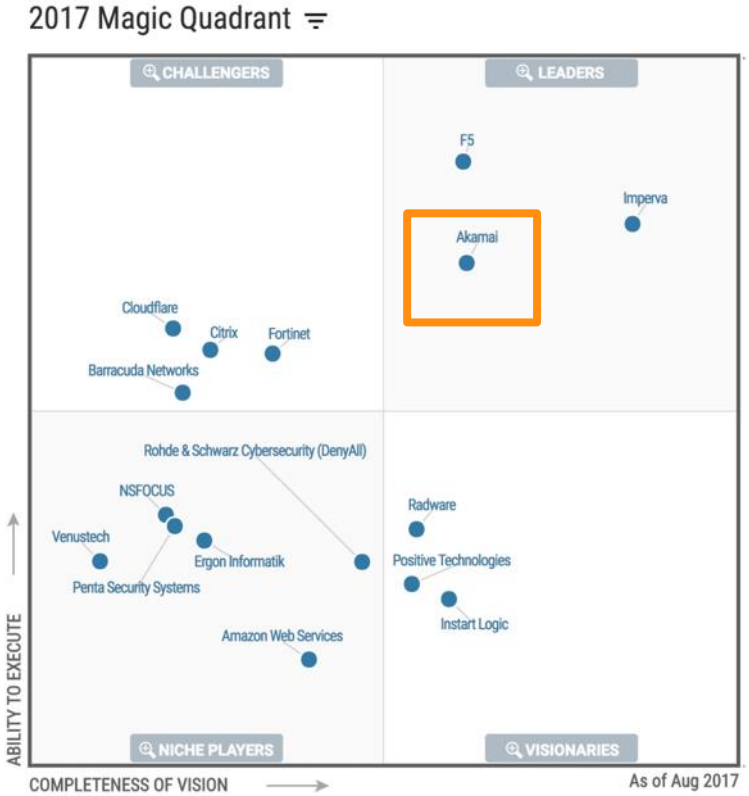
Mehr als 18 Jahre Erfahrung



©2017 AKAMAI

Akamai

Gartner: Akamai im Leader Quadrant für WAF*



* Web Application Firewall

Source:
Magic Quadrant for
Web Application Firewalls,
Gartner (August 2017)

Gartner unterstützt keine der Anbieter, Produkte oder Dienste, die in seinen Forschungspublikationen erwähnt werden, und rät Technologienutzern nicht, nur die Anbieter mit den höchsten Bewertungen oder sonstigen Attributen auszuwählen. Forschungspublikationen von Gartner geben die Ansichten der Gartner-Forschungsabteilung wieder und sollten nicht als Tatsachenbehauptungen verstanden werden. Gartner schließt jegliche ausdrückliche oder stillschweigende Gewährleistung in Bezug auf diese Forschung aus, einschließlich Gewährleistungen der Handelsüblichkeit oder Eignung für einen bestimmten Zweck.

OWASP Top 10 RC1 - 2017

- A1 – Injection
- A2 – Broken Authentication
- A3 – Cross-Site Scripting
- A4 – Broken Access Control
- A5 – Security Misconfiguration
- A6 – Sensitive Data Exposure
- A7 – Insufficient Attack Protection
- A8 – Cross-Site Request Forgery
- A9 – Using Components with Vul.
- A10 – Under protected APIs

©2017 AKAMAI

Akamai

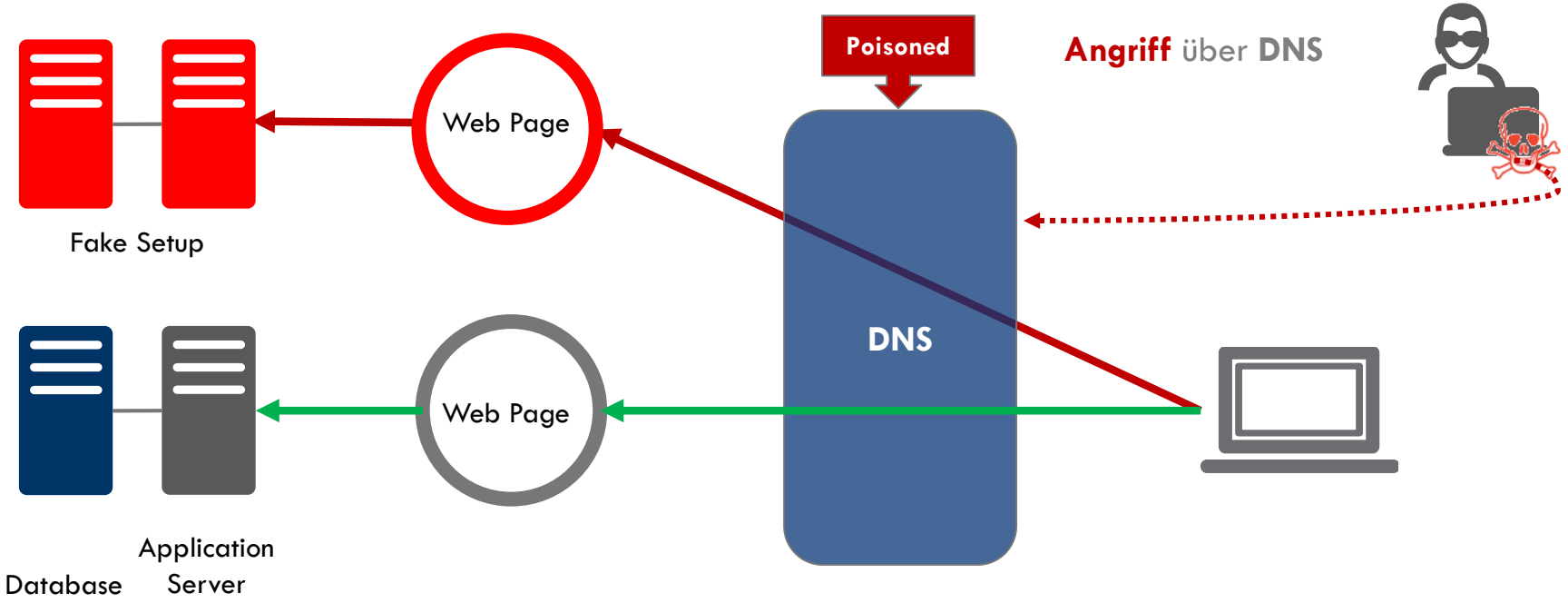
OWASP Top 10 RC2 – Okt. 2017

- A1 – Injection
- A2 – Broken Authentication
- A3 – Sensitive Data Exposure
- A4 – XML External Entities
- A5 – Broken Access Control
- A6 – Security Misconfiguration
- A7 – Cross-Site Scripting
- A8 – Insecure Deserialization
- A9 – Using Components with Vul.
- A10 – Insufficient Logging & Mon.

©2017 AKAMAI

Akamai

Angriffe auf persönliche Daten

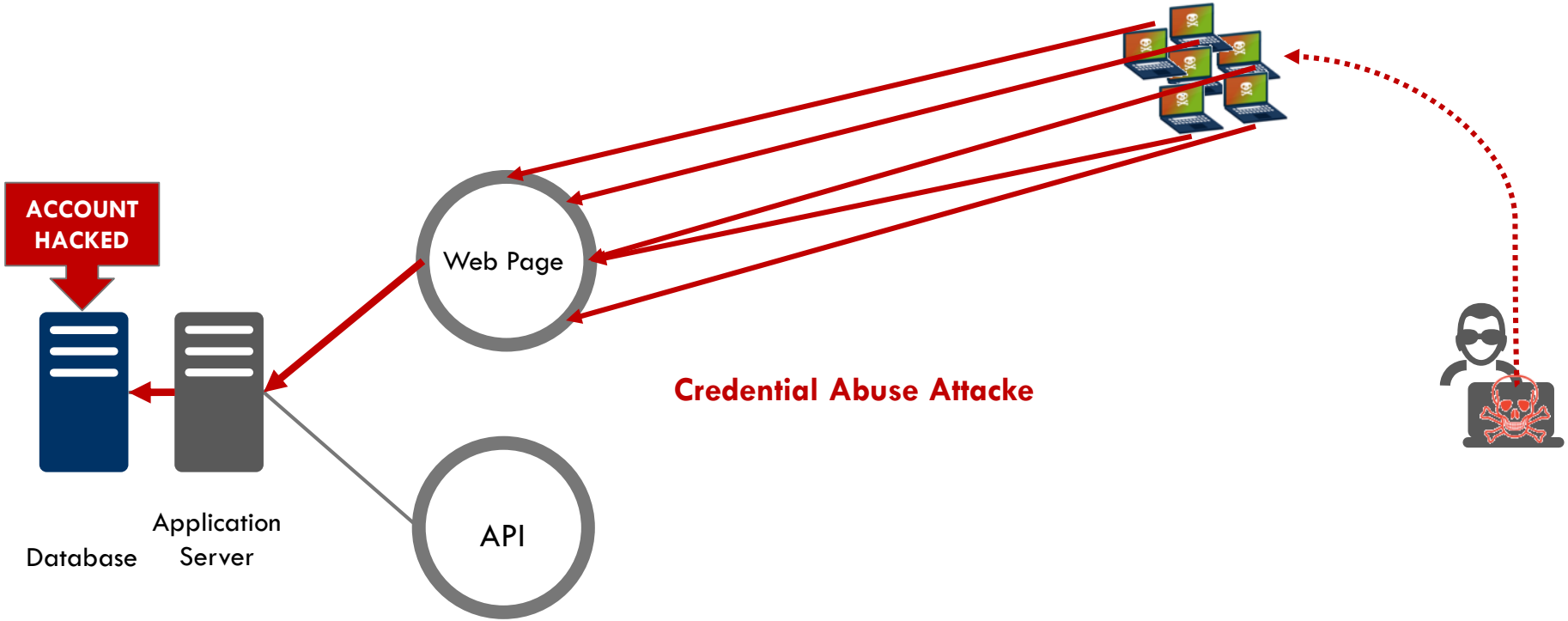


©2017 AKAMAI

Angriffe auf persönliche Daten

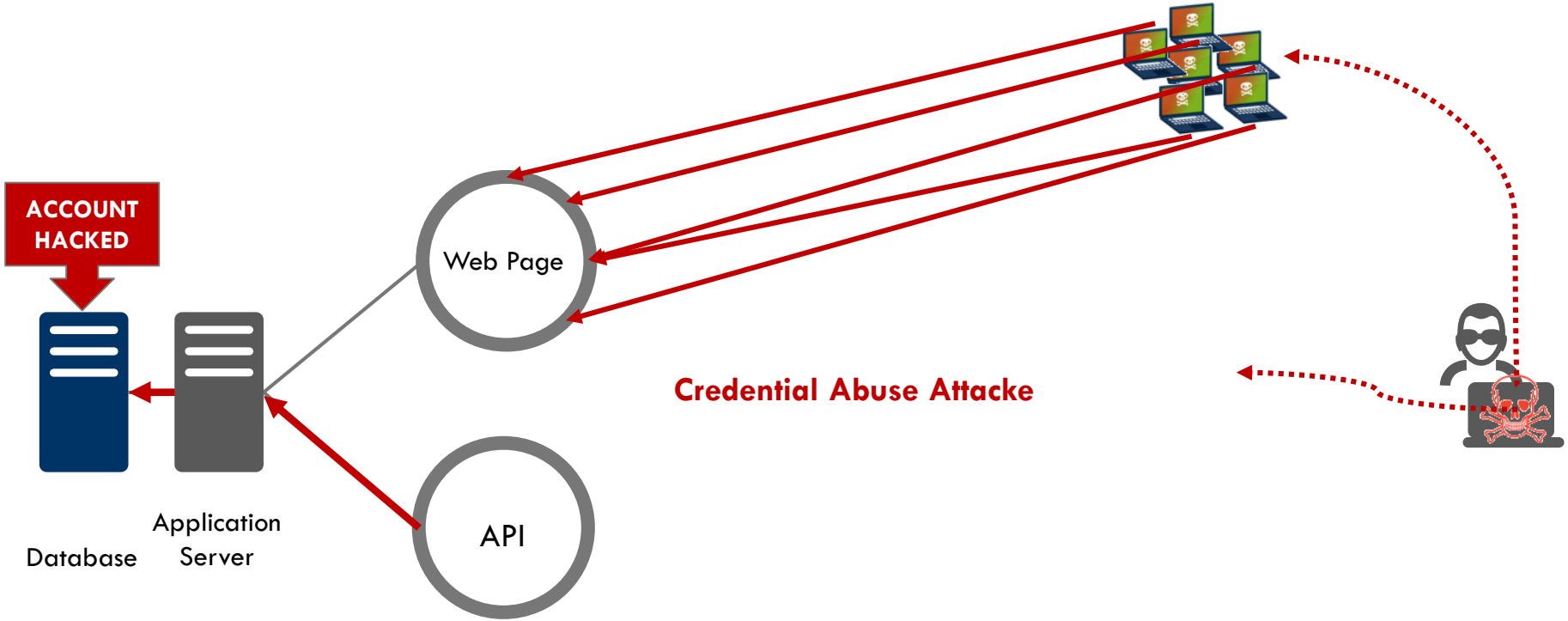
©2017 AKAMAI

Angriffe auf persönliche Daten



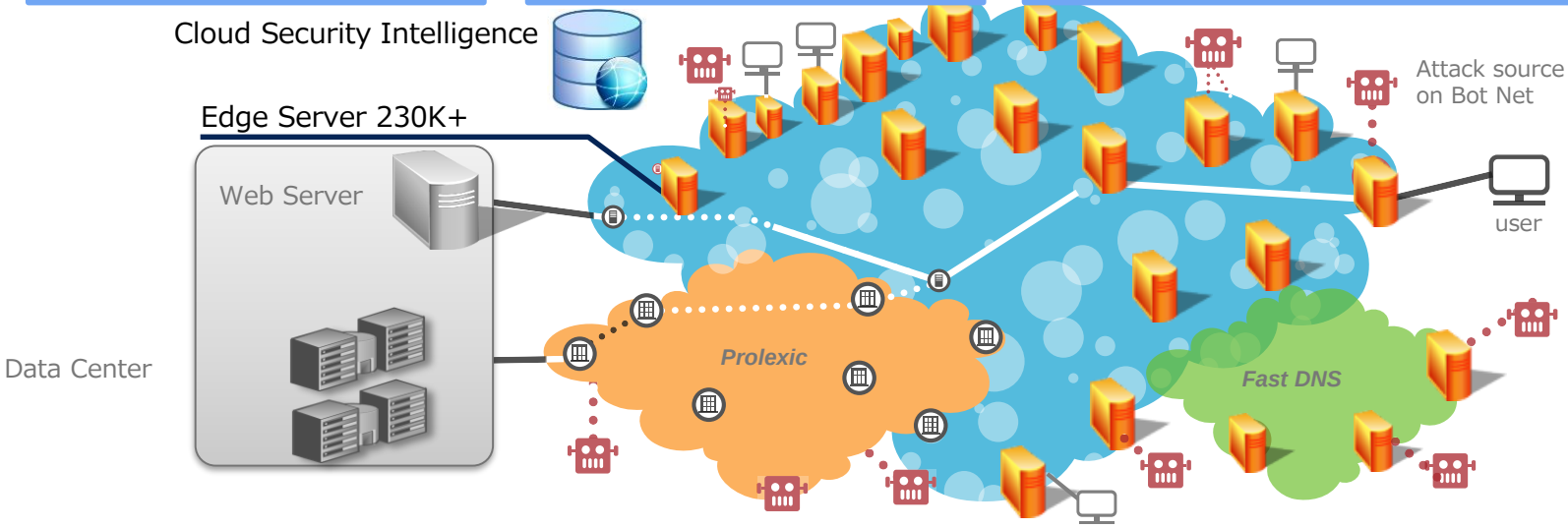
©2017 AKAMAI

Angriffe auf persönliche Daten



Akamai Cloud Security Solution

Bot Manager	Client Reputation	Kona Site Defender
Detect Anomaly Bot and Control request/response from Bot.	Using reputation information from Cloud Security Intelligence to protect from malicious source.	Integrated web security solution, protect customer Origin from DDoS / Web Attacks.



Prolexic	Fast DNS
Protect from DDoS attacks Data Center level.	Highly distributed authoritative DNS service to protect from DDoS attacks.

Akamai Cloud Security Solution – DSGVO

Bot Manager

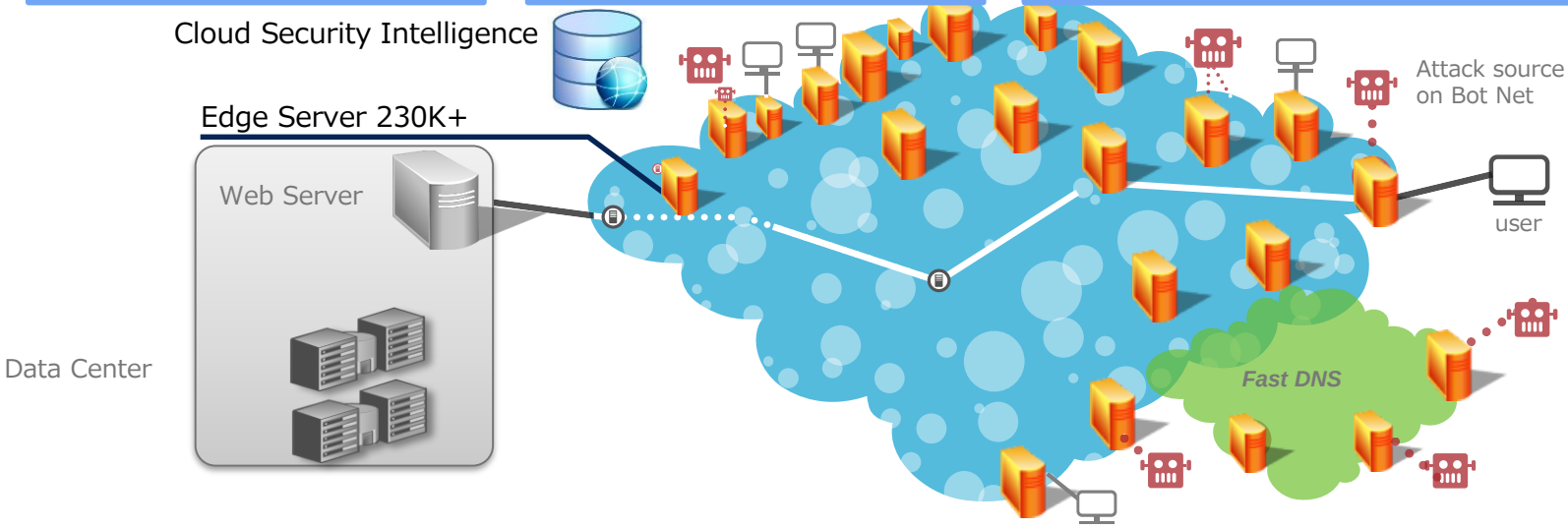
Detect Anomaly Bot and Control request/response from Bot.

Client Reputation

Using reputation information from Cloud Security Intelligence to protect from malicious source.

Kona Site Defender

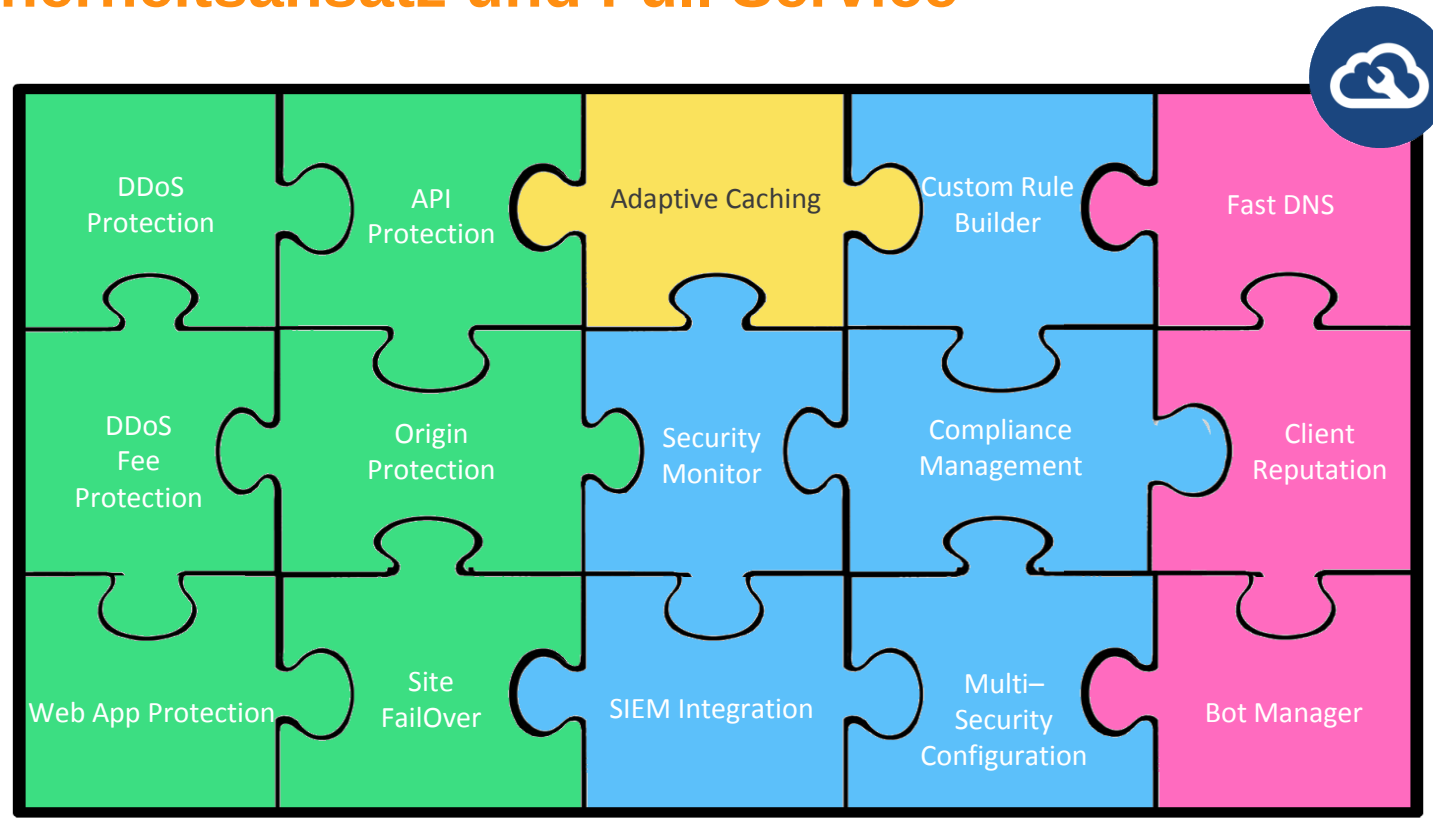
Integrated web security solution, protect customer Origin from DDoS / Web Attacks.



Fast DNS

Highly distributed authoritative DNS service to protect from DDoS attacks.

Sicherheitsansatz und Full Service



Managed

©2017 AKAMAI

Vielen Dank!

Gerne beantworten wir Ihre Fragen.