praemandatum

16.04.2015 praemandatum GmbH

“Leckeres aus dem Labor“

bei praemandatum

Einleitung

- praemandatum heute
- Portfolio

Das Laboratorium

- Grundidee
- Unterschiedliche Arten

Aus der Reihe „Was wir Ihnen gerne ersparen würden“

Unser Angebot

- Security by Design
- Beratung, Beratung, Beratung

Zusammenfassung

praemandatum

- Ausgründung der Leibniz-Universität Hannover
  - Gründung Februar 2008
  - Heute: etwa 30 Personen
- Expliziter Fokus auf Datenvermeidung
  - Technisch, juristisch, emotional – aus einer Hand
- (Wahrsch.) die ersten dieser Berufsgattung
  - Dadurch starke Medienpräsenz

praemandatum

- Ausgründung der Leibniz-Universität Hannover
  - Gründung Februar 2008
  - Heute: etwa 30 Personen
- Expliziter Fokus auf Datenvermeidung
  - Technisch, juristisch, emotional – aus einer Hand
- (Wahrsch.) die ersten dieser Berufsgattung
  - Dadurch starke Medienpräsenz
  - Guter Ruf und gute Referenzen
  - Publikation in Fach- und Massenmedien

KONICA MINOLTA
SENNHEISER
ADG
VDE
ROLAND
DEKRA Akademie GmbH
DEKRA
Alles im grünen Bereich.
Datenschutz PRAXIS
DAT Datenschutz aktuell
Frankfurter Allgemeine
ZEITUNG FÜR DEUTSCHLAND
COMPUTER+UNTERRICHT

praemandatum

- Ausgründung der Leibniz-Universität Hannover
  - Gründung Februar 2008
  - Heute: etwa 30 Personen
- Expliziter Fokus auf Datenvermeidung
  - Technisch, juristisch, emotional – aus einer Hand
- (Wahrsch.) die ersten dieser Berufsgattung
  - Dadurch starke Medienpräsenz
  - Guter Ruf und gute Referenzen
  - Publikation in Fach- und Massenmedien

Portfolio

- Akademie
  - **Audits**
    - Datenvermeidung und Datenschutz für Unternehmen
    - Datenvermeidung und Datenschutz für Geheimnisträger
    - Topologiecheck
    - Topologie- und Netzwerkscan
    - Clientcheck
    - Servercheck
  - **Seminare**
    - Mitarbeitersensibilisierung
      - Wo ist das Internet / Neue Technologien
      - Angriffspunkte der IT Infra
      - Smartphones/ Apps/ BYOD
      - Schadmails, Passwörter, Verschlüsselung
      - Social Engeneering
    - IT-Kompetenzseminar Datensicherheit
    - Schulung für System-Administratoren
    - Für Führungskräfte mit Weitblick
- Laboratorium

Einleitung

- praemandatum heute
- Portfolio

Das Laboratorium

- Grundidee
- Unterschiedliche Arten

Aus der Reihe „Was wir Ihnen gerne ersparen würden“

Unser Angebot

- Security by Design
- Beratung, Beratung, Beratung

Zusammenfassung

Grundidee des Laboratoriums

- Entwicklung von Datenvermeidungs- und Datenschutzkonzepten
- Von allen Seiten integrativ betrachtet:
  - Konzeption
  - Soft- und Hardware
  - Gedrucktes und Prozesse
  - Vertrieb
  - Marketing
  - Betriebswirtschaft
  - Juristisches

Projektarten

- Intrinsische Projekte
  - Aus eigenen Ideen entstehen Konzepte
  - Wir bieten Marktteilnehmern in hart umkämpften Branchen **proaktiv** ein Alleinstellungsmerkmal an
  - Datenschutz funktioniert als solches derzeit überraschenderweise gut...

- Extrinsische Projekte
  - Entwicklung auf direkte Nachfrage von Kunden

Einleitung

- praemandatum heute
- Portfolio

Das Laboratorium

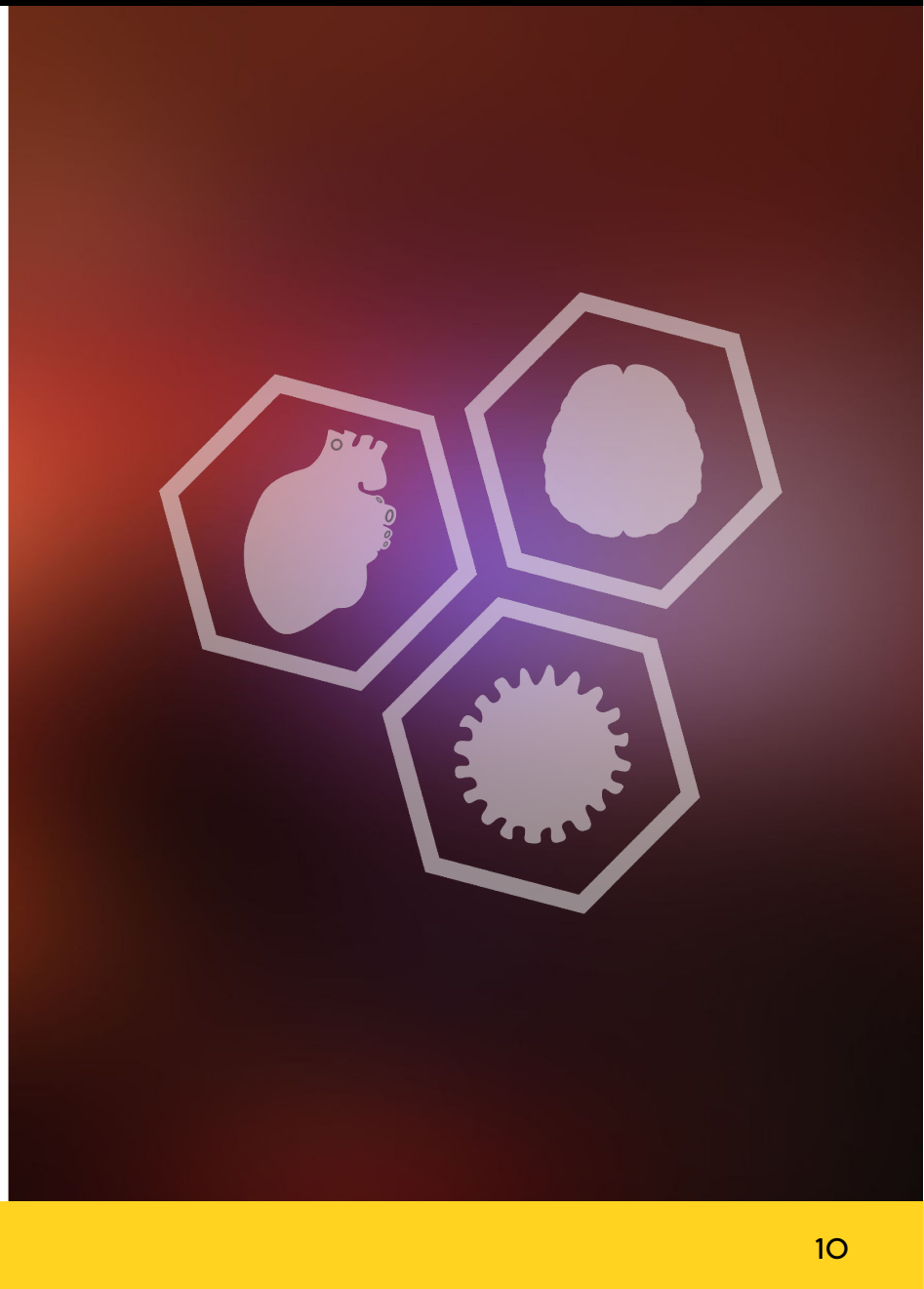
- Grundidee
- Unterschiedliche Arten

Aus der Reihe „Was wir Ihnen gerne ersparen würden“

Unser Angebot

- Security by Design
- Beratung, Beratung, Beratung

Zusammenfassung



Aus der Reihe:

„Was wir Ihnen gerne ersparen würden“

Heute:

„Immer Ärger mit Certificate Authorities“

oder

„Warum https nur die halbe Miete ist“

Jüngst in der Presse

- Lenovo und Superfish – Adware Man-in-the-Middle
- Google entdeckt wiederholt gefälschte Zertifikate
- Finnischer Spaßvogel lässt sich Microsoft-Zertifikat ausstellen
- …

Erinnern Sie sich noch?

Certificate Authority???

- CAs beglaubigen Authentizität
- Bindet öffentlichen Schlüssel an Identität → Zertifikat
- Beispiel https://praemandatum.de
  - Aussteller (Issuer): Thawte, Inc.
  - Bescheinigt: Inhaberschaft der Domain praemandatum.de
  - Frage 1: Wie hat Thawte das geprüft?
  - Frage 2: Vertrauen Sie Thawte?
  - Bonus: Was heißt wohl **`Basic Constraints: CA:FALSE`** ?

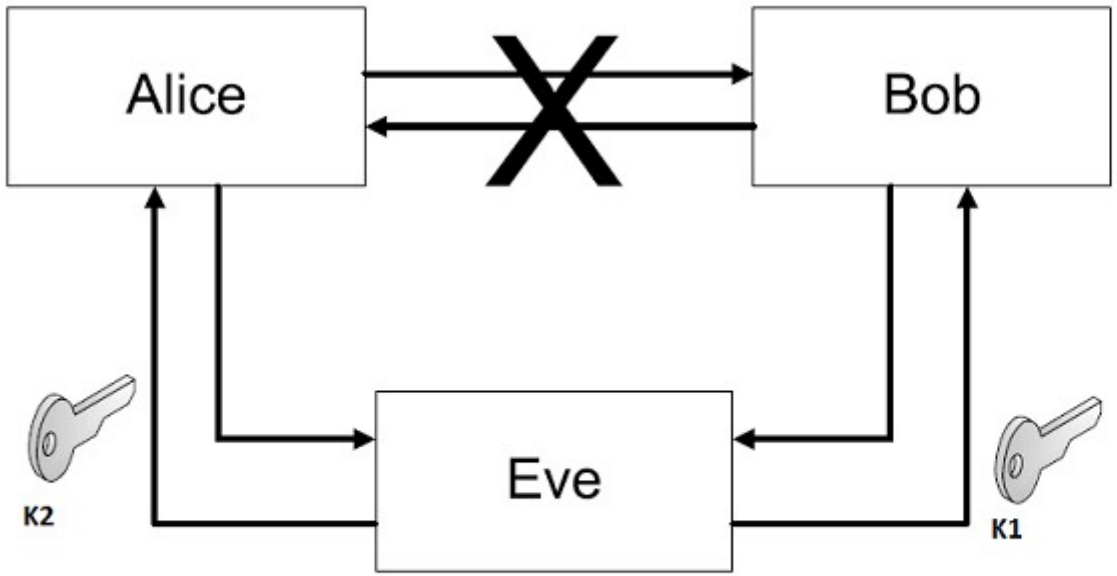
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:  5a:[...]:88
    Signature Algorithm: [...]
        Issuer: C=US, O=Thawte, Inc.,
                OU=Domain Validated SSL,
                CN=Thawte DV SSL CA
        Validity
            Not Before: Jul 10 2014 GMT
            Not After : Jul 10 2015 GMT
        Subject: CN=praemandatum.de
        Subject Public Key Info:
            Public Key Algorithm: rsa
                Public-Key: [...]
            X509v3 Basic Constraints:
                CA:FALSE

    Signature Algorithm: sha256WithRSA

         […]:7f:3d:1a:8b
```

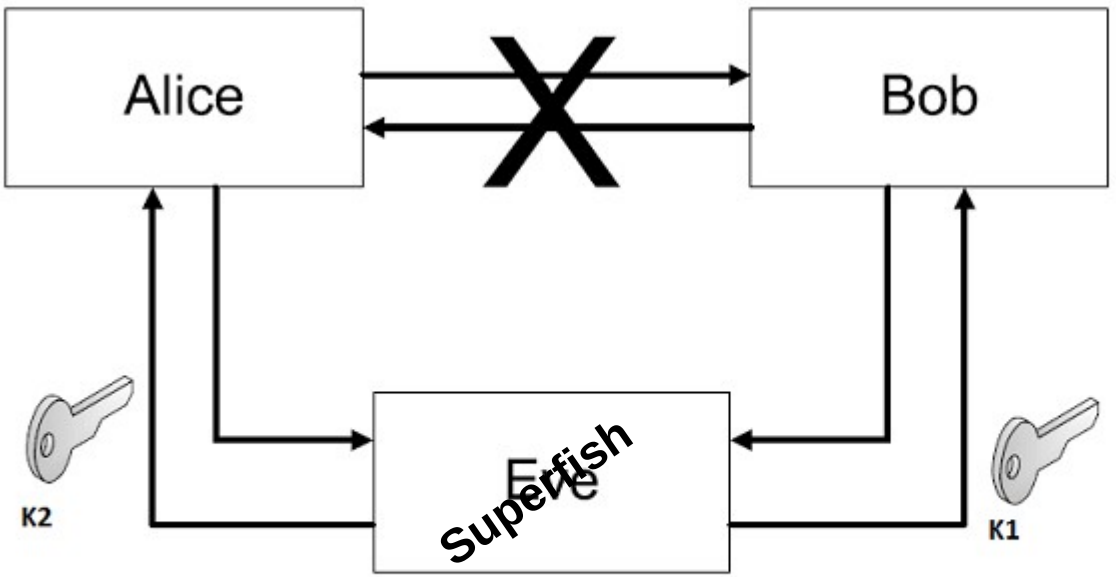
Wozu das alles?

- Um Authentizität zu erreichen
  - Ohne Authentizität auch keine Vertraulichkeit
    → Man-in-the-Middle-Angriffe (MITM)



Lenovo feat. Superfish Visual Discovery

- Auf Lenovo-Geräten vorinstallierte Adware
- Funktion
  - Fängt http und https-Kommunikation des Nutzers ab und blendet Werbung in die Antworten der Webserver ein



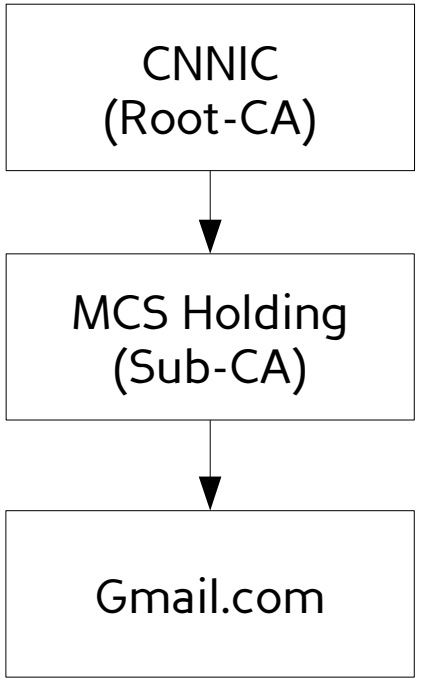
Lenovo feat. Superfish – es geht noch schlimmer

- Superfish-CA bei Lenovo-Rechnern als vertrauenswürdig eingetragen
- Superfish liefert geheimen Schlüssel der CA gleich mit
  → offenes Scheunentor für Man-in-the-Middle und Phishing

- Lessons learned:
  Hätte Lenovo doch bloß jemand mit Ahnung gefragt...

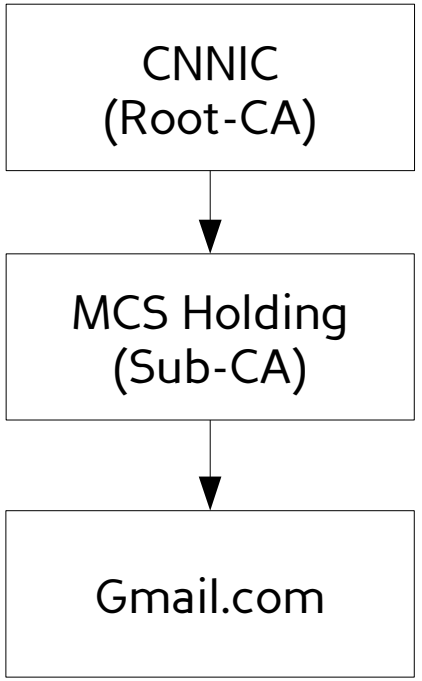
Google findet gefälschte Zertifikate

- Google hat Probleme des CA-Systems schon lange erkannt
  - Chrome hat Fingerabrücke der offiziellen Google-Zertifikate fest eingestellt,
  - Chrome erkennt somit illegitime Google-Zertifikate
  - und meldet diese...
- Jüngste Entdeckung:
  CNNIC beglaubigt indirekt illegitime Google-Zertifikate
  - MCS verwendet Sub-CA unerlaubt für ihre MITM-Produkte
  - Google listet CNNIC aus



Google findet gefälschte Zertifikate

- Lessons learned:
  - Sub-CAs potenzieren die Undurchsichtigkeit des CA-Systems
  - Certificate Pinning gehört in jedes neue Produkt
- Preisfrage:
  Wie viele Sub-CAs gibt es wohl?



Finne hat Spaß mit Microsoft-Zertifikat

- Es geht auch ohne China und Sub-CAs:
  Finnischer IT-Experte registiert Mailadresse *hostmaster@live.fi*
  - Registrierung habe er zum Spaß versucht und es klappte
  - Nächster Schritt: Zertifikat für *live.fi* bei COMODO ausstellen lassen
    → Domain Validation per E-Mail erfolgreich
    - BTW: Comodo ist der Marktführer für TLS/SSL-Zertifikate
  - Microsoft hat Hinweise des IT-Experten ignoriert

- Lessons learned:
  - Es gibt viele Gelegenheiten sich gegenüber den Big-Playern positiv abzugrenzen

Einleitung

- praemandatum heute
- Portfolio

Das Laboratorium

- Grundidee
- Unterschiedliche Arten

Aus der Reihe „Was wir Ihnen gerne ersparen würden“

Unser Angebot

- Security by Design
- Beratung, Beratung, Beratung

Zusammenfassung

Unser Angebot

- Security by Design
  - Wir arbeiten mit an Ihrer Produktentwicklung
  - Stand der Technik und darüber hinaus
- Produkt schon fertig?
  - Wir machen Audits
  - Memos
- Klassische Beratung
  - Expertisen
  - Marktanalysen
  - Bei Geschäftsabschlüssen

Einleitung

- praemandatum heute
- Portfolio

Das Laboratorium

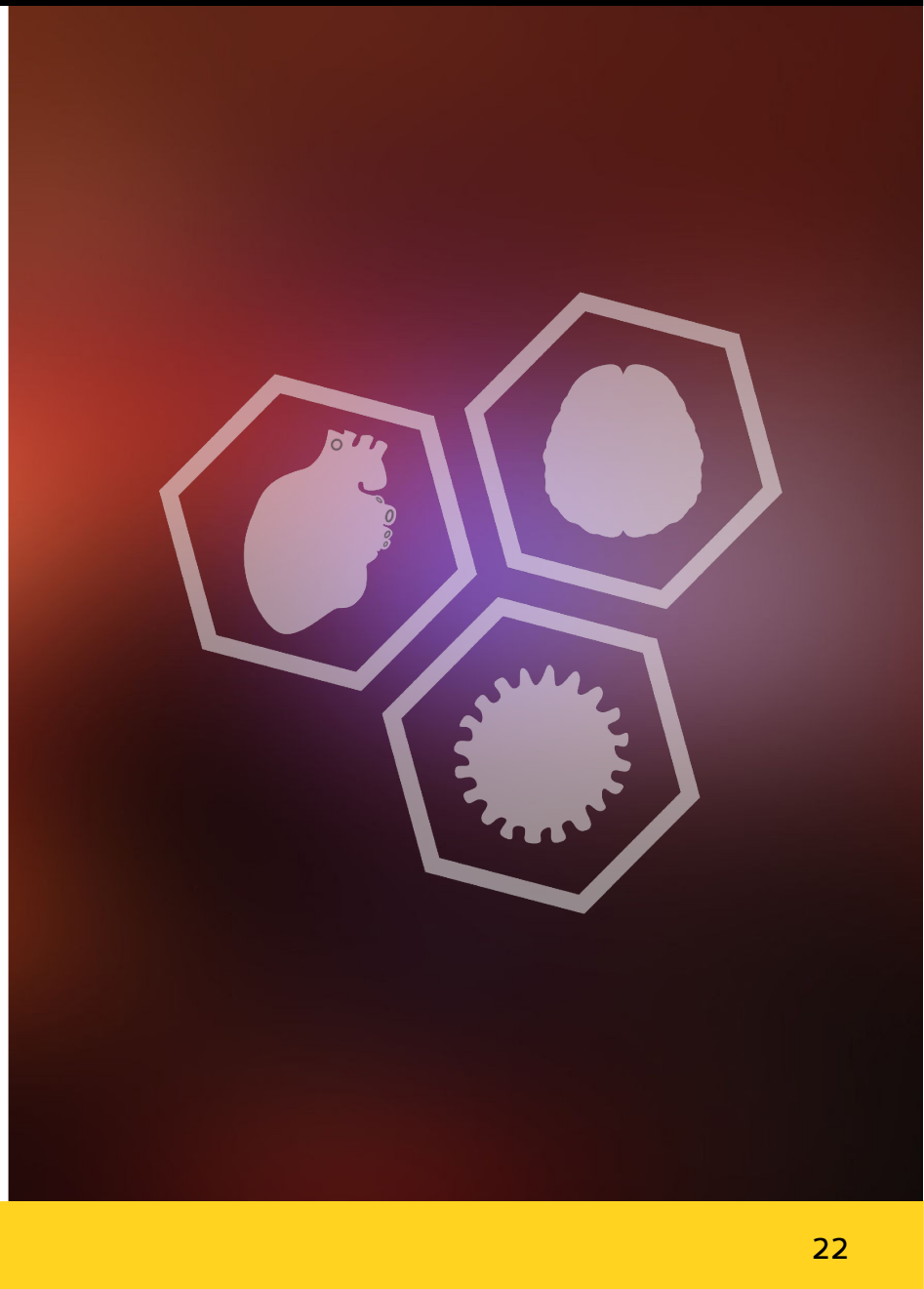
- Grundidee
- Unterschiedliche Arten

Aus der Reihe „Was wir Ihnen gerne ersparen würden“

Unser Angebot

- Security by Design
- Beratung, Beratung, Beratung

Zusammenfassung



Zusammenfassung

- Worum es geht
  - Technischer Datenschutz und Datenvermeidung sind die großen Themen der kommenden Jahre
  - praemandatum macht genau dies länger als alle anderen
  - Nutzen der günstigen Aufmerksamkeitslage, bekanntmachen des Unternehmens
  - Geordnete Entwicklung von entsprechenden Produkten und Konzepten „in Serie“, Wachstum
- Was wir haben
  - Passendes Personal, Know-How, auch absehbar keine Recruitingprobleme („Sexinessfaktor“)
  - Guten Ruf, gute Referenzen, relativ hohen Bekanntheitsgrad in der Branche, gute Kontakte

16.04.2015 praemandatum GmbH

“Leckeres aus dem Labor“

bei praemandatum

kontakt@praemandatum.de

Tel.: 0511 – 96 94 98 600

Weiterführende Links

- Lenovo Superfish http://heise.de/-2554455
- Gefälschte Google-Zertifikate http://heise.de/-2583414
- Microsoft-Zertifikat ohne Prüfung ausgestellt http://heise.de/-2576861
- Gogo Man-in-the-Middle im Flugzeug http://heise.de/-2512310
- Firefox Add-on Certificate Patrol Mozilla Add-ons
- Defcon-Vortrag: SSL and the Future of Authentication
- Electronic Frontier Foundation: SSL Obervatorium