IT-Sicherheit

DI Dr. Harald Kornfeil
EDV-Referent ÄK-Sbg
30.01.2024

IT-Sicherheit

- Was muss geschützt werden?

  im Kontext des Arztes v.a.

  personenbezogene Daten

  (Patientendaten = Gesundheitsdaten = sensible Daten, Mitarbeiterdaten, Kundendaten)

  aber auch Wirtschafts-/Finanzdaten, Gehälter, ...

- Was sind *personenbezogene* Daten?

  „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen, etwa Name, Adresse, Geburtsdatum, E-Mail-Adresse, IP-Adresse, Kontonummer“

  https://www.oesterreich.gv.at/lexicon/D/Seite.991455.html

IT-Sicherheit

- Datensicherheit
  - Wie verarbeite ich meine Daten?
  - Wer hat Zugriff auf (welche) Daten?
  - Wie sichere ich meine Daten?
- Kommunikationssicherheit
  - Wie versende ich meine Daten?
  - Wem sende ich meine Daten?
  - Welche Daten sende ich?

Gefahren für die Datensicherheit?

- Die „Elemente“
  - Stromausfall / Gewitter
- Hardwareausfall
- Netzwerkausfall
- „Schädling“ von Außen (= „Hacker“)
  - Spyware / Ransomware
- „Schädling“ von Innen (= „User“)

Was hilft?

Backup!

Was noch?

- Die „Elemente“
  - Stromausfall / Gewitter
- Hardwareausfall
- Netzwerkausfall
- „Schädling“ von innen (aka „User“)
  - Spyware / Ransomware
- „Schädling“ von außen (aka „Hacker“)

evtl. USV/Überspannungsableiter

evtl. Reservehardware/Servicevertrag

evtl. Firewall / Virenscanner / Updates

Schulung !

Schulung !

... aber letztlich hilft nur

Backup!

Backup!

Backup!

Backup!

Backup!

Kommunikationssicherheit

- Telefon (Mithören, VOIP!)
- Fax (ab 1.1.2025 nicht mehr erlaubt!)
- Digitale Befundübertragung
- eMail (nur wenn verschlüsselt!)
- Messenger
  - DSGVO-**No-Go**: Whats-app, Telegram
  - DSGVO-**OK**: Signal, Threema, Matrix (Element.io)
- Post

Was hat das mit ELGA/eCard zu tun?

Wir sind für den Schutz der Patientendaten verantwortlich ...

... und zwar auch die, die in der ELGA liegen!

Was muss/kann/soll ich tun?

Awareness und Schulung

- ***Selbst***
  - weiterbilden
  - konsequent sein
- ***Mitarbeiter***
  - weiterbilden / schulen
  - aufpassen

Wie wird angegriffen?

Heutzutage *kaum mehr* ***direkter*** Angriff auf ein Netzwerk von Außen

- selten ein Computer direkt mit Internet verbunden
- meist ein Netzwerk mit Firewall (und NAT)
  (Achtung: Umstellung auf IPv6 könnte/wird das ändern!)

ABER:

- unsichere WLANs und veraltete Router/Firewalls

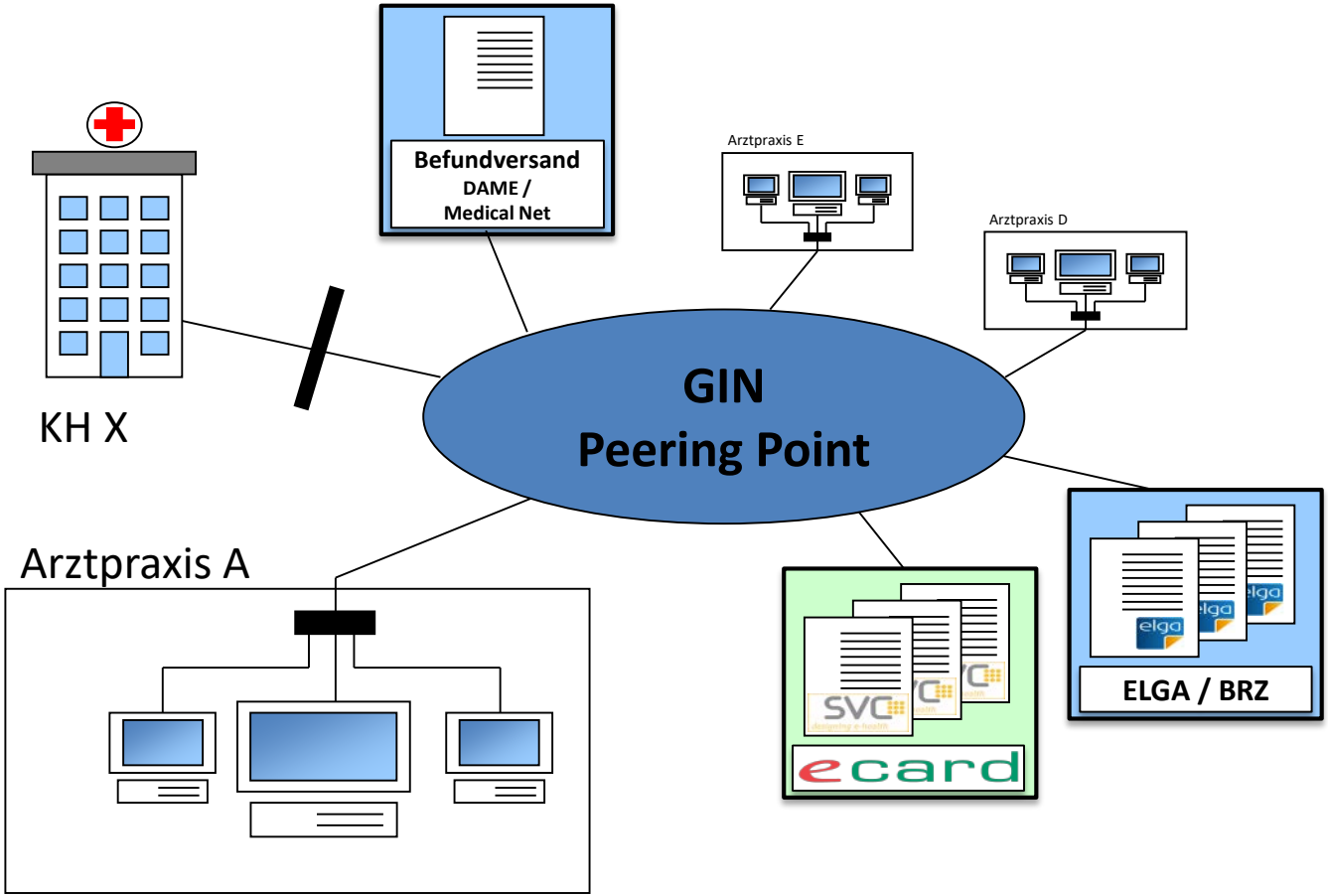
Einfallstore für Schadsoftware

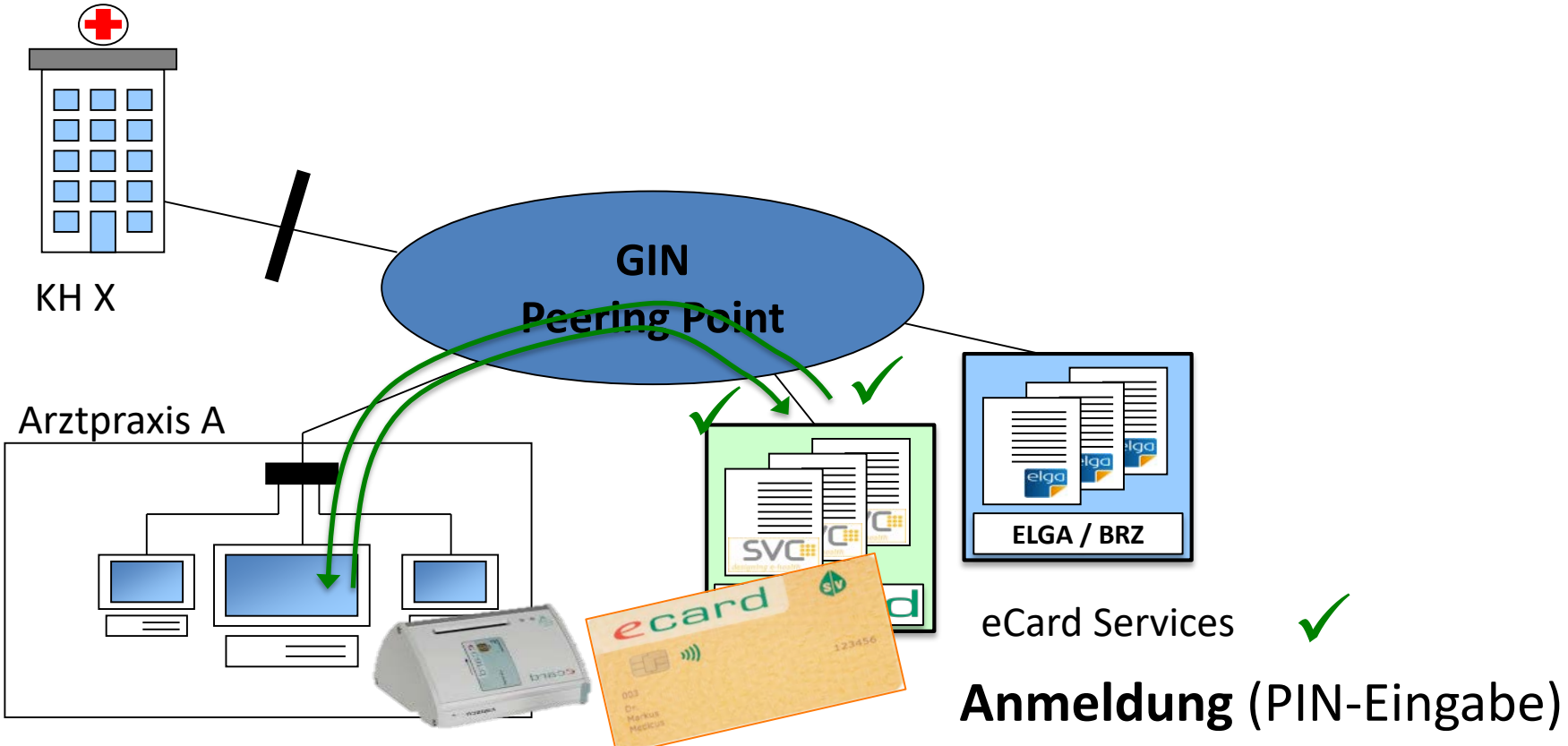
- Drive-By
- Phishing
- Netzwerkzugang (= Ethernet-Buchsen) in Praxis-Räumen
- unsicheres WLAN
- USB-Ports bei Rechnern
- Tastatur
  - Bildschirmschoner / Bildschirm sperren (Windows-L)
  - Passwort für angemeldeten User (Fingerprint-Mouse)

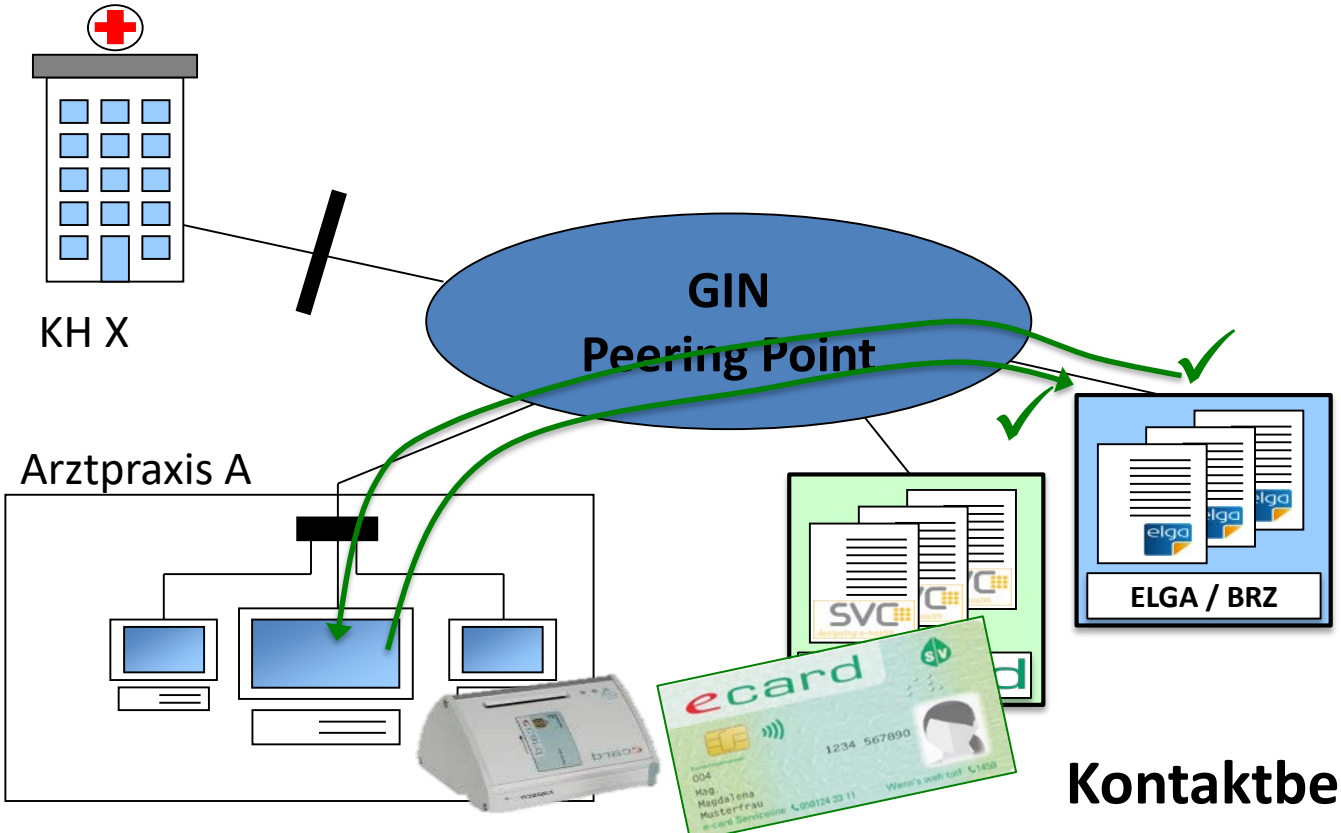
Allgemeiner Netzaufbau

eines Ordinations-LAN mit eCard-Anschluss

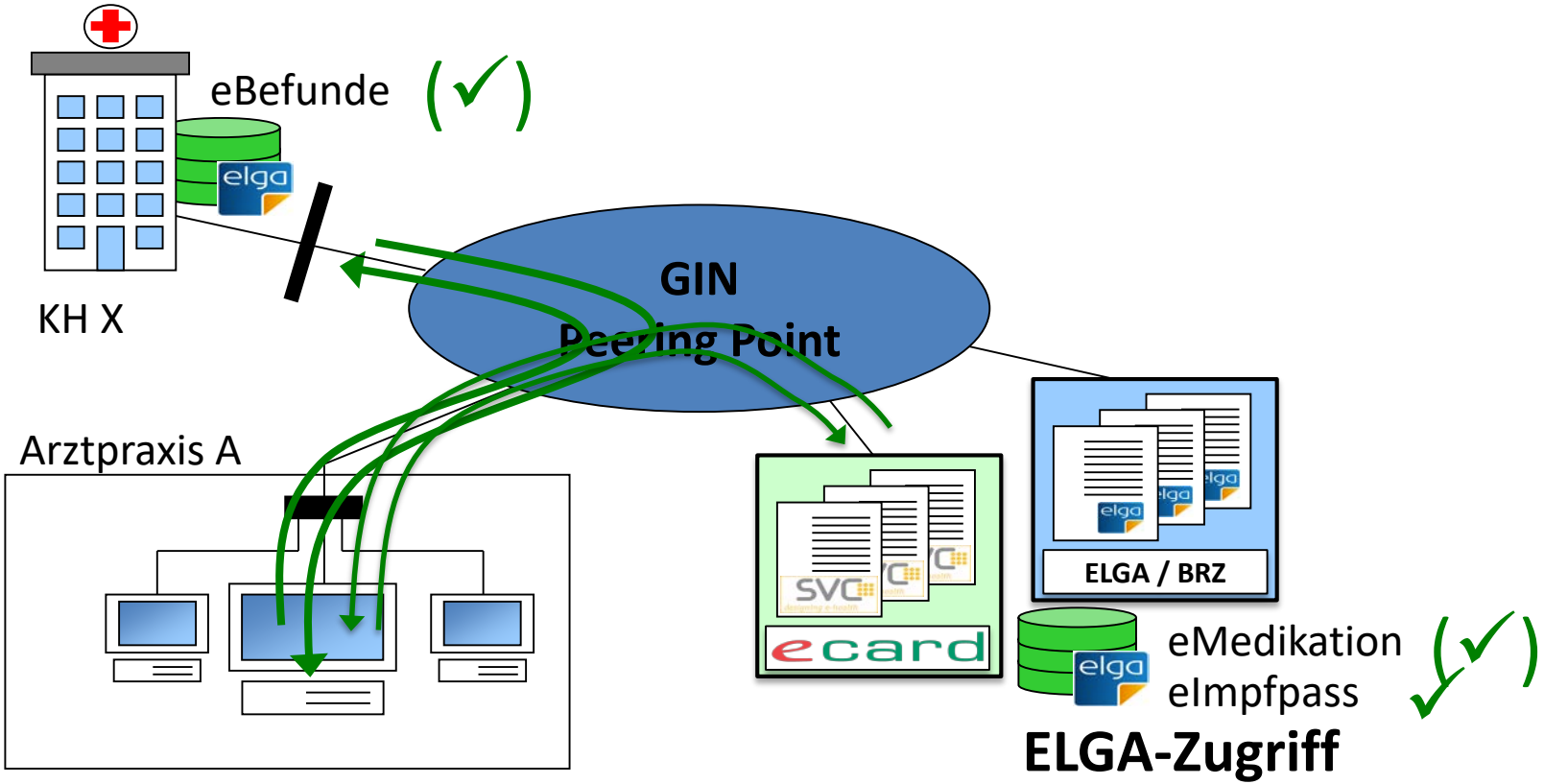
mit GIN-Verbindung (WAN)


Befundversand
DAME /
Medical Net
Arztpraxis E
Arztpraxis D
KH X
GIN
Peering Point
Arztpraxis A
SVC
ecard
elga
ELGA / BRZ


KH X
GIN
Peering Point
Arztpraxis A
ELGA / BRZ
eCard Services
Anmeldung (PIN-Eingabe)



Kontaktbestätigung

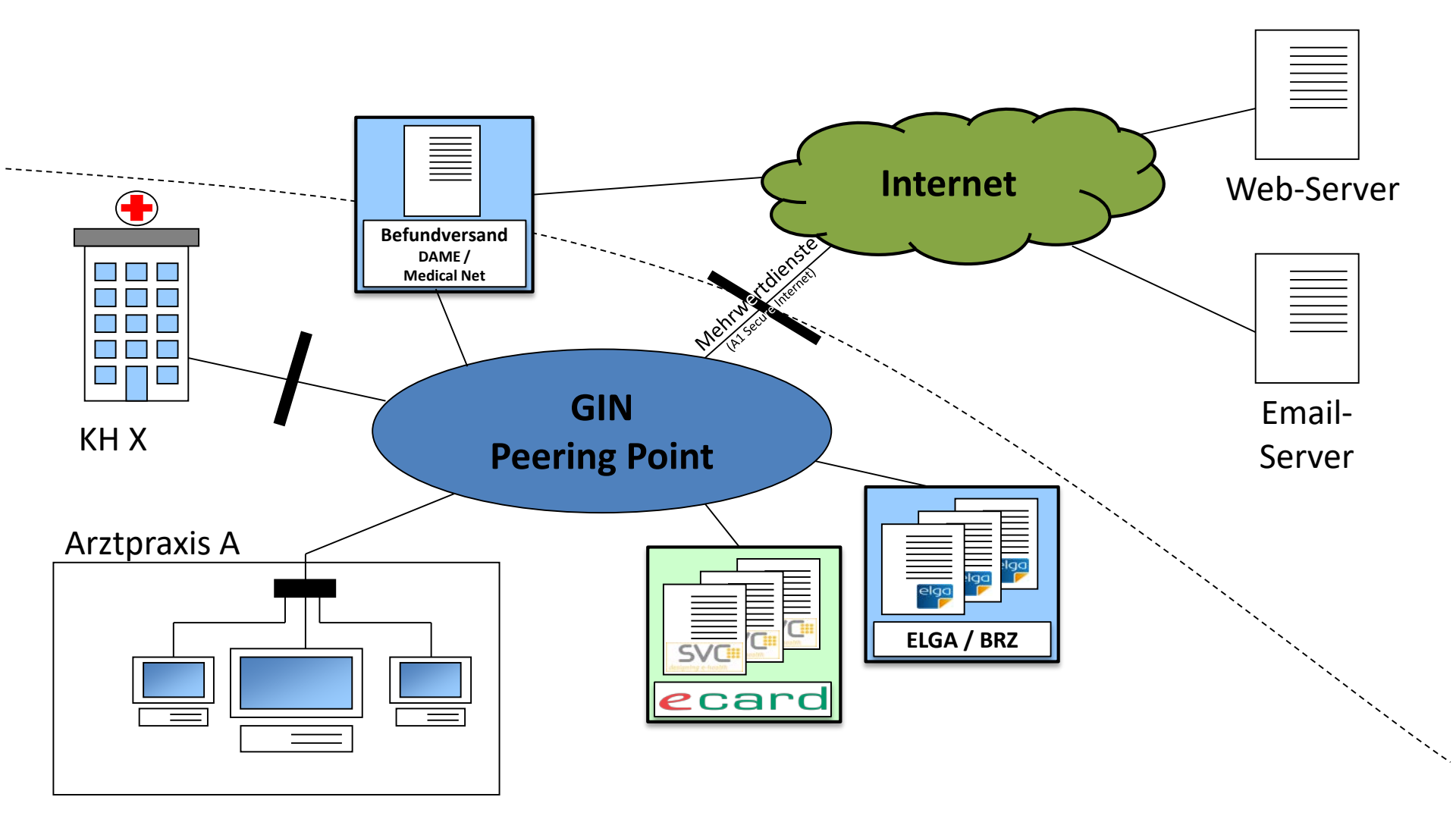

eBefunde
KH X
GIN
Peering Point
Arztpraxis A
ELGA / BRZ
ecard
eMedikation
eImpfpass
ELGA-Zugriff

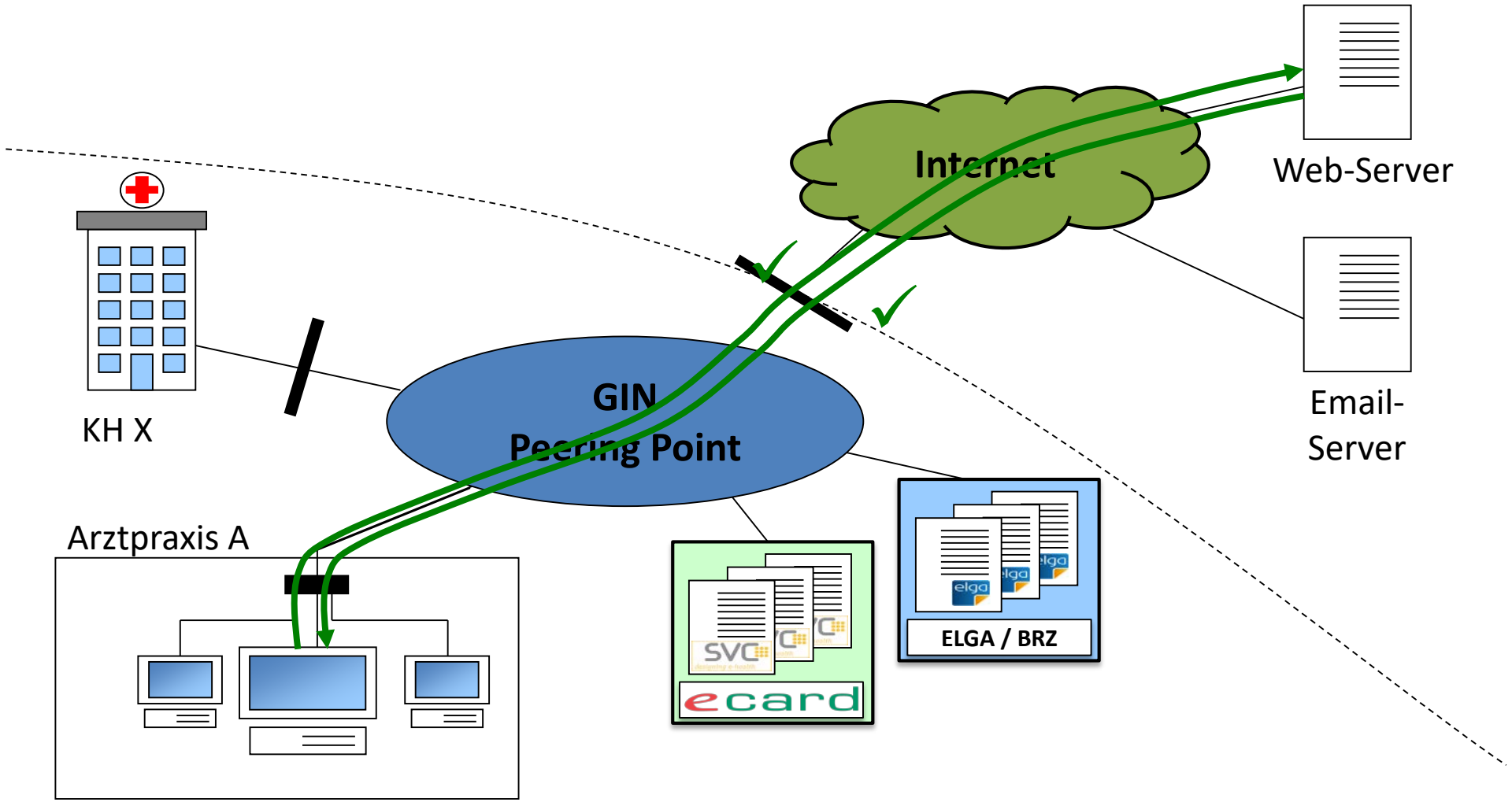
Netzaufbau

Scenario 1

Ordination **mit** eCard-Anschluss

und Internet-Verbindung via GIN-Router


Befundversand
DAME /
Medical Net
Internet
Web-Server
Mehrwertdienste
(A1 Secure Internet)
KH X
GIN
Peering Point
Email-
Server
Arztpraxis A
ELGA / BRZ
ecard

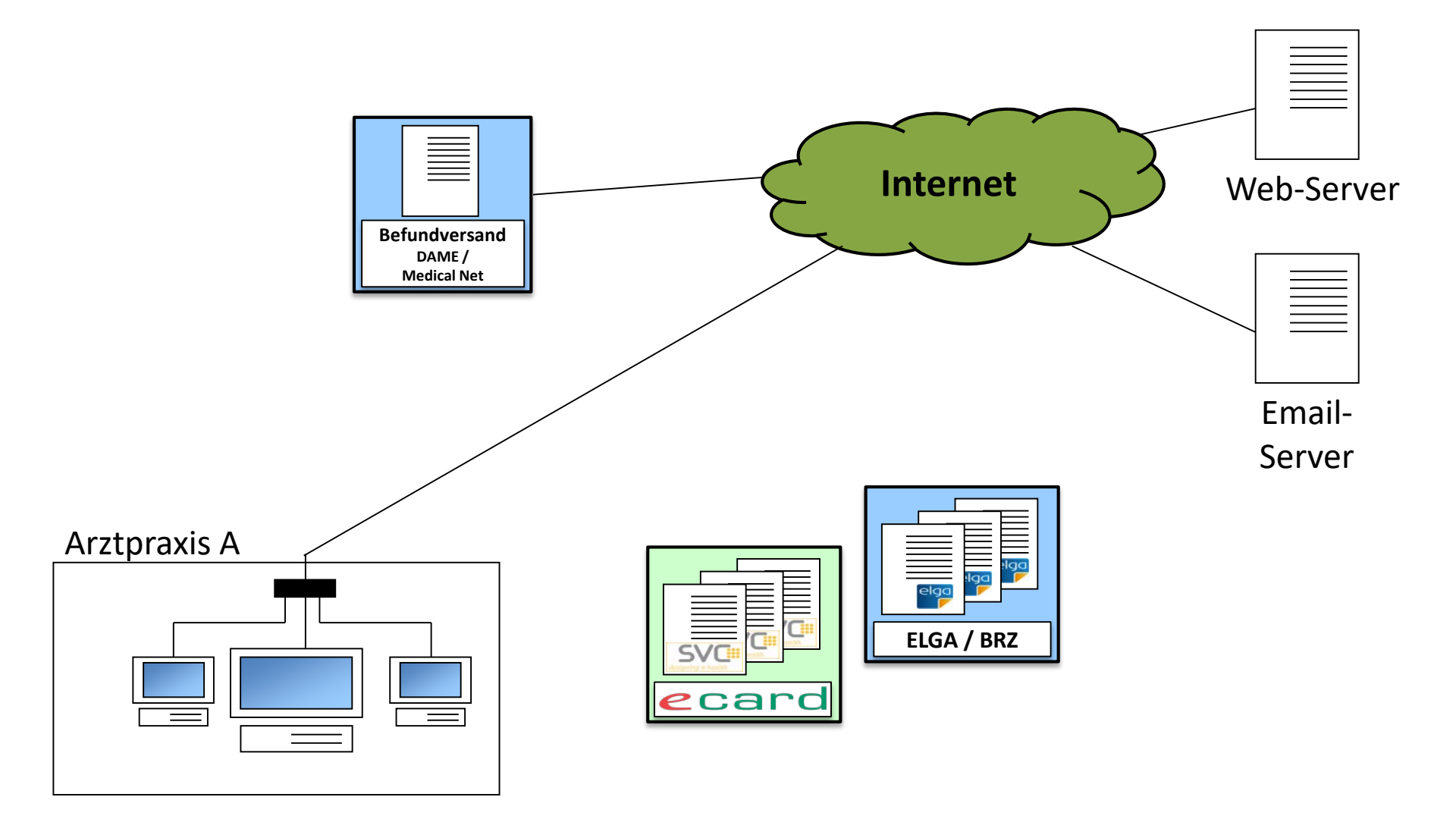

Internet
Web-Server
Email-
Server
KH X
GIN
Peering Point
Arztpraxis A
SVC
ecard
elga
ELGA / BRZ

Netzaufbau

Scenario 2

(Wahlarzt)-Ordination **ohne** eCard-Anschluss

mit Internet-Verbindung


Befundversand
DAME /
Medical Net
Internet
Web-Server
Email-
Server
Arztpraxis A
SVC
ecard
elga
ELGA / BRZ

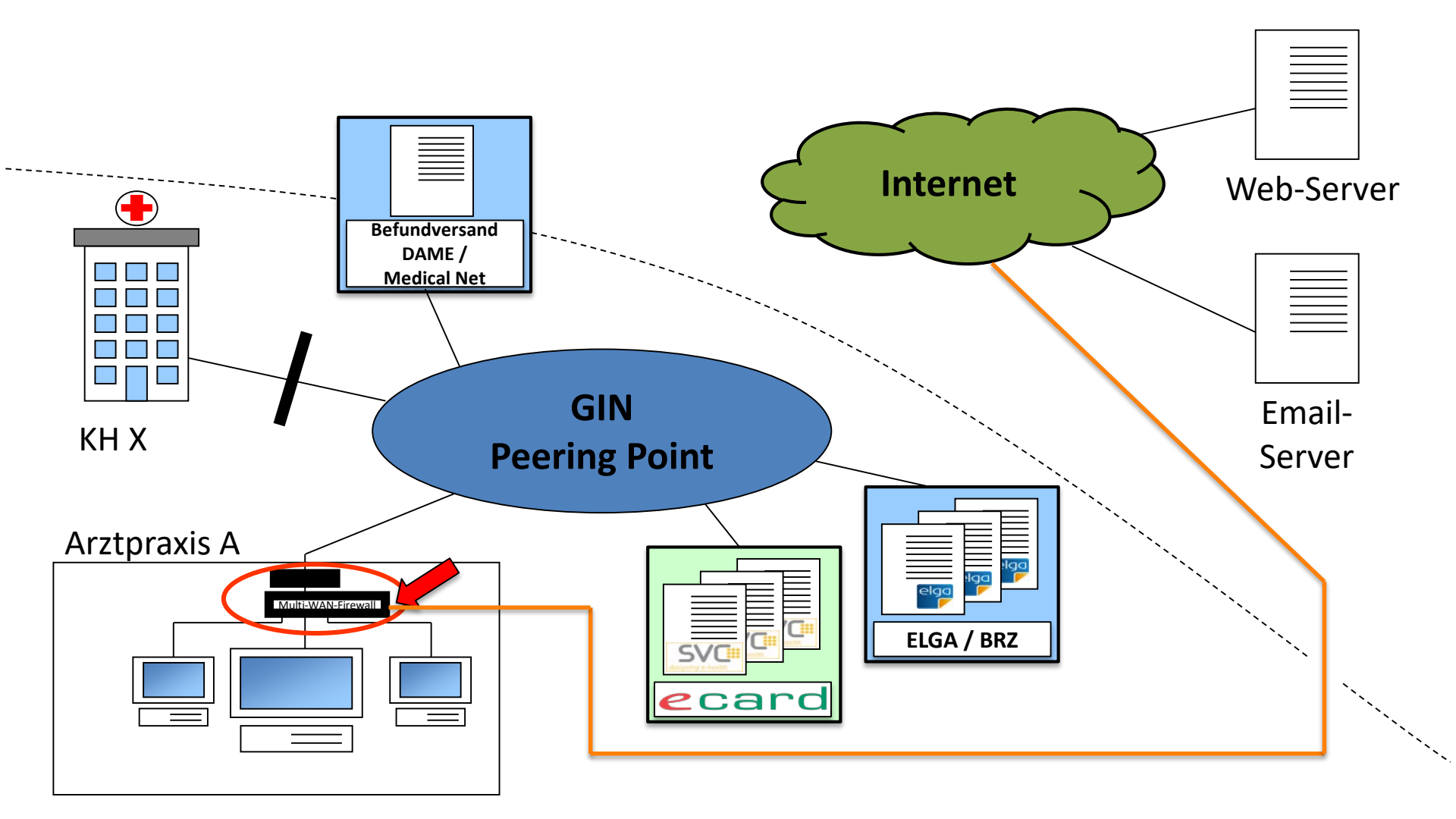
Netzaufbau

Scenario 3

Ordination **mit** eCard-Anschluss

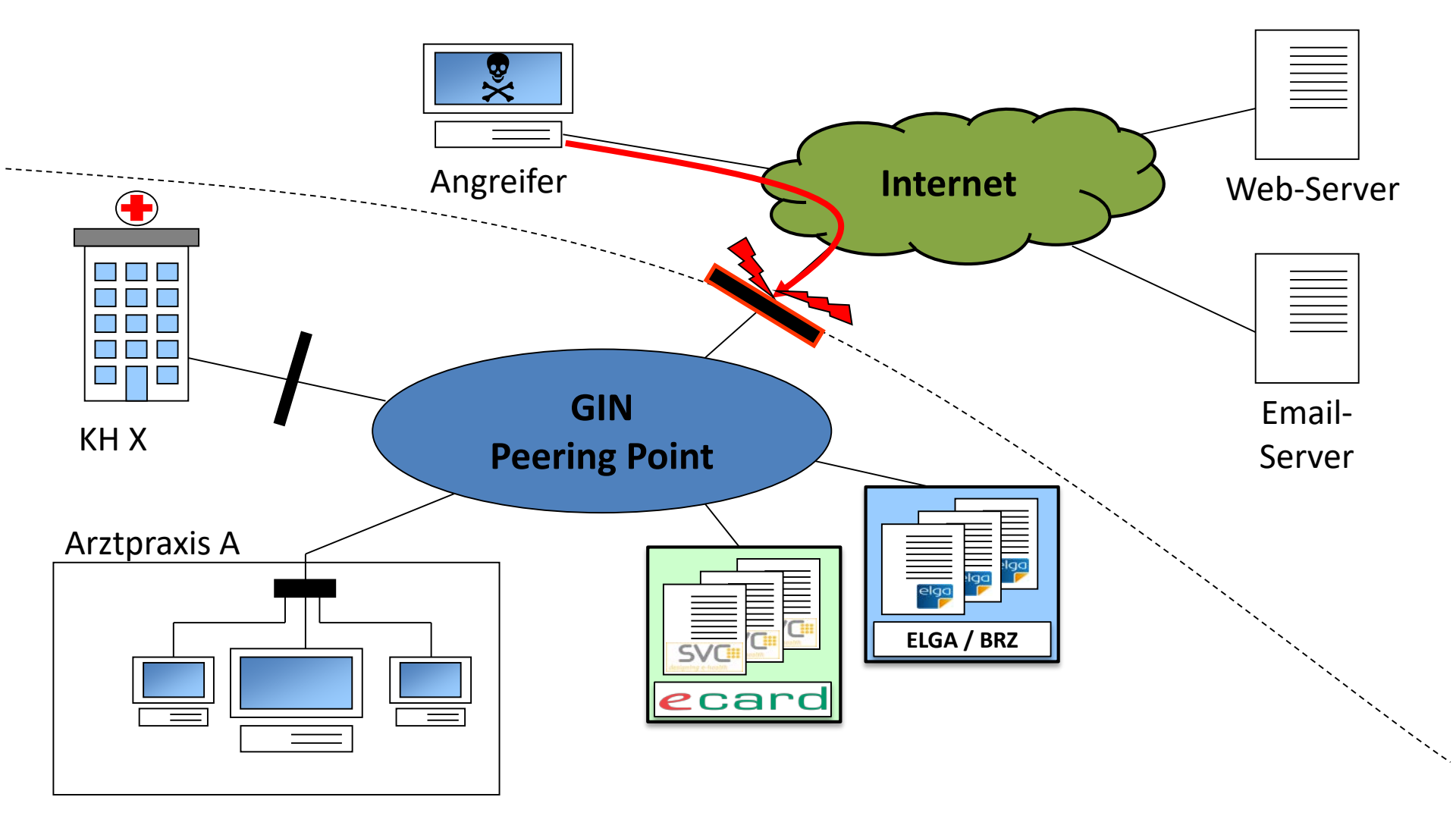
und 2. Netzanschluss ins Internet

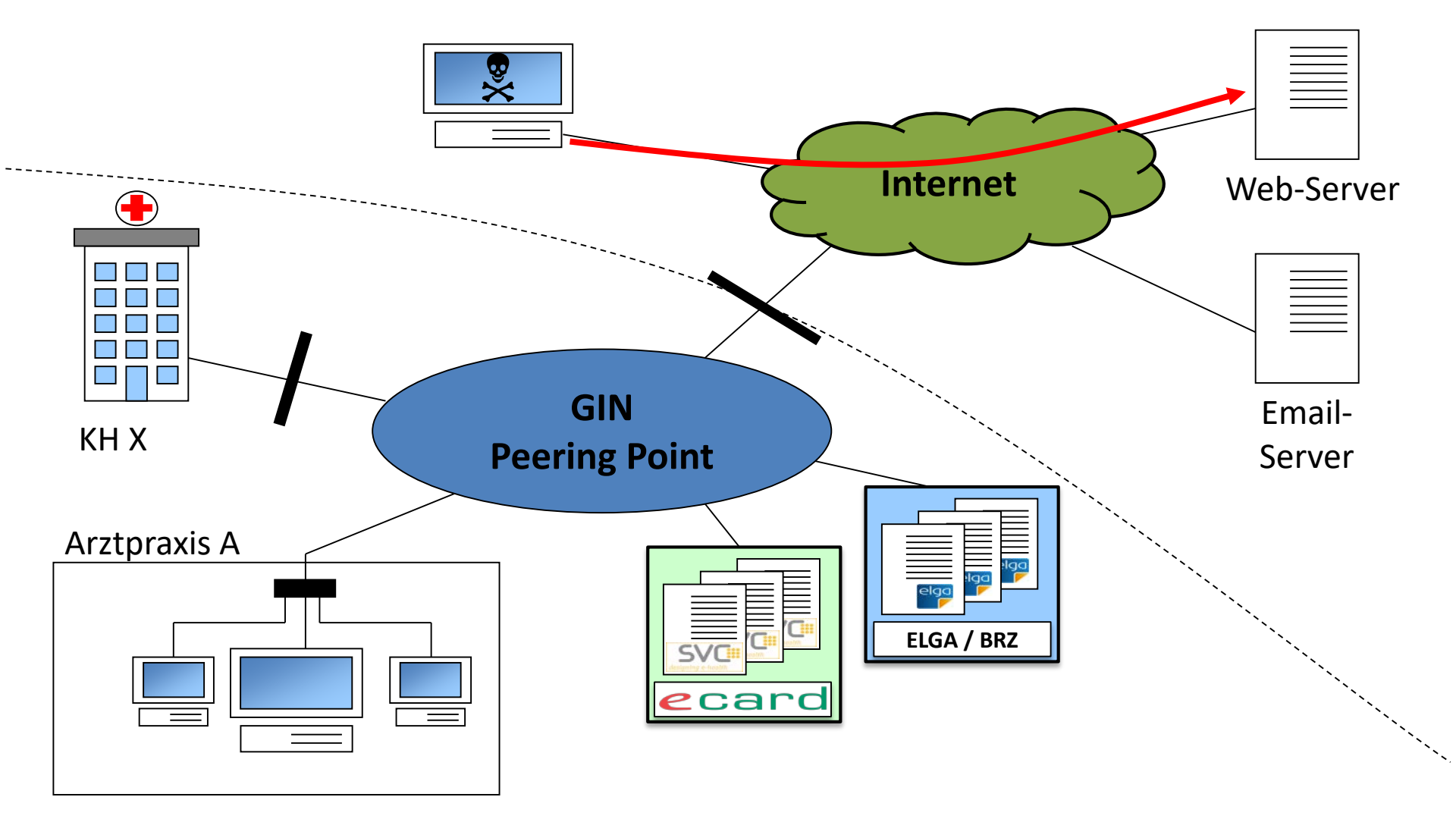
z.B. f. Praxisvernetzung, Außenzugriff (Home-Office, Visiten-Laptop)

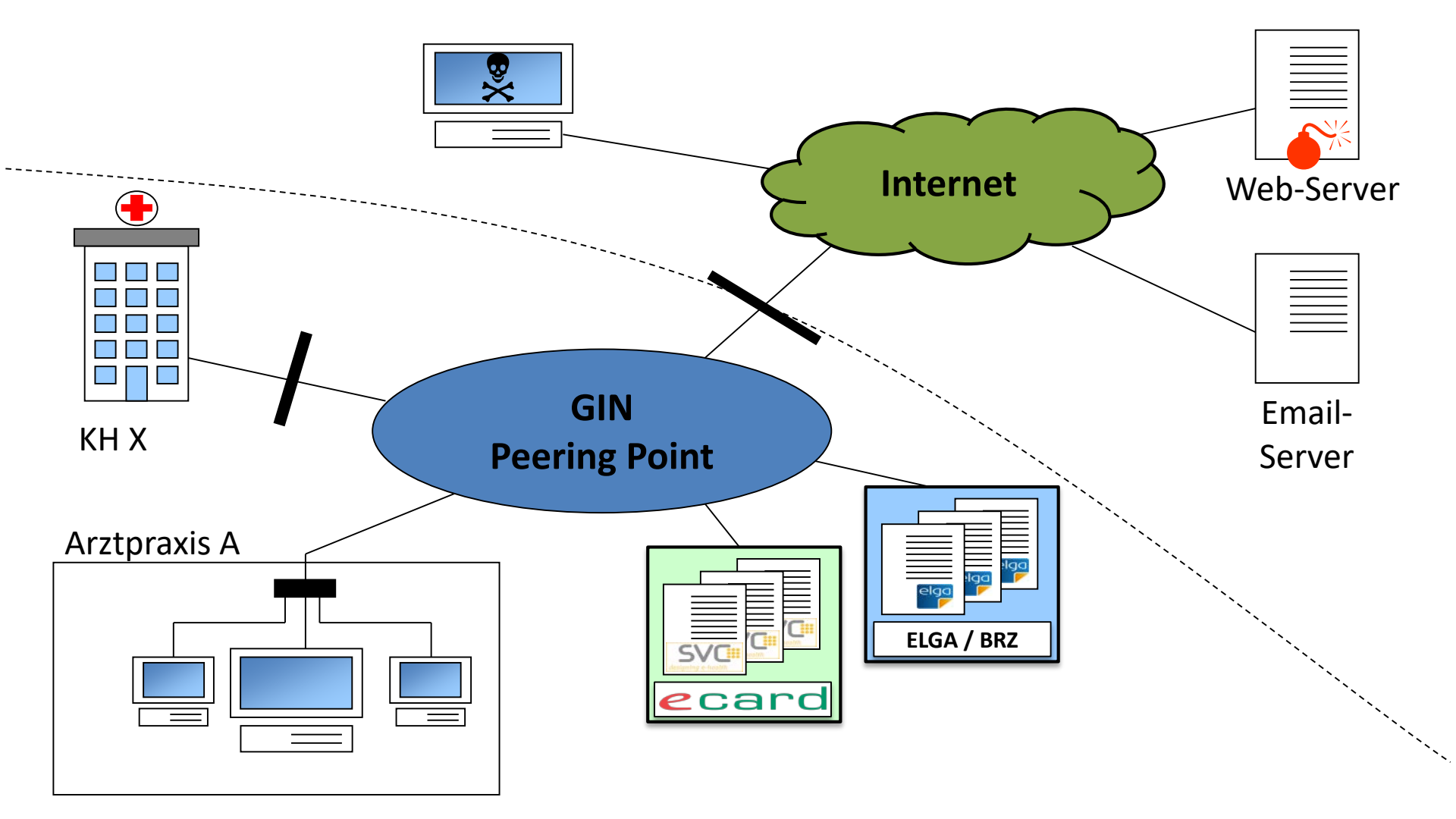

Befundversand
DAME /
Medical Net
Internet
Web-Server
KH X
GIN
Peering Point
Email-
Server
Arztpraxis A
Multi-WAN-Firewall
SVC
ecard
elga
ELGA / BRZ

Angriffs-Schritt 1

Hacken des Web-Servers


Angreifer
Internet
Web-Server
Email-
Server
KH X
GIN
Peering Point
Arztpraxis A
ELGA / BRZ
ecard

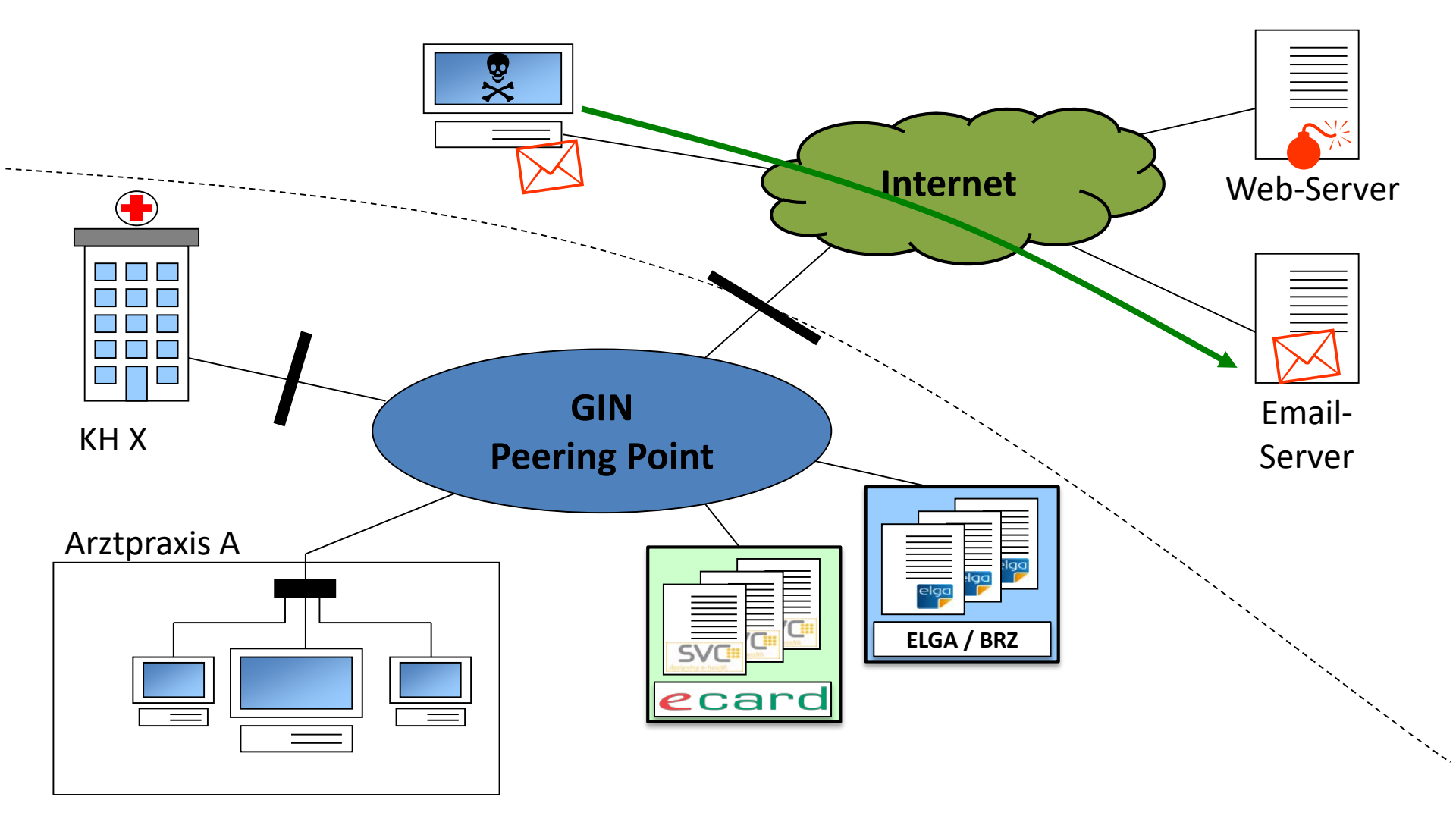

Internet
Web-Server
Email-
Server
KH X
GIN
Peering Point
Arztpraxis A
ELGA / BRZ
ecard

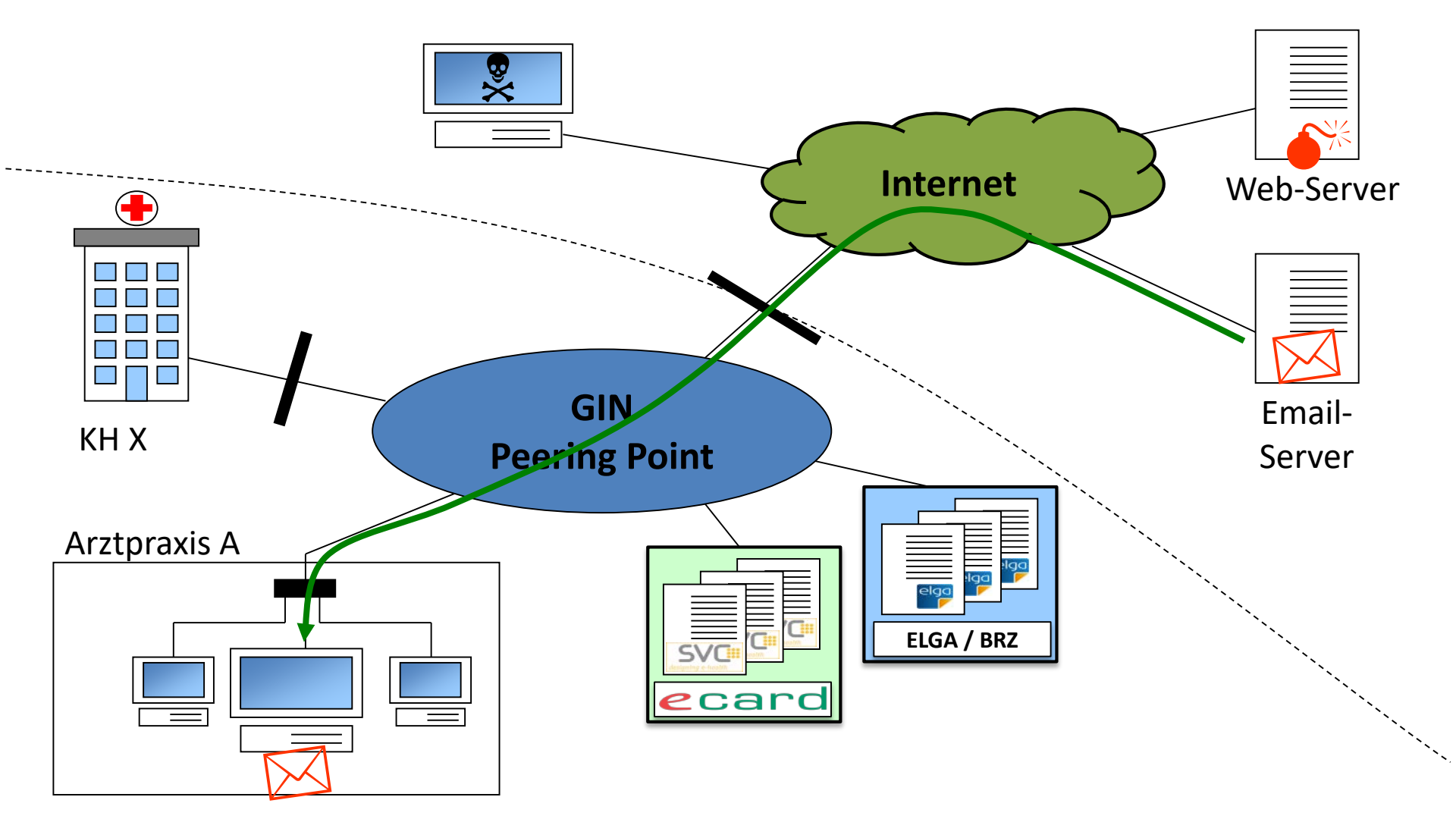

Internet
Web-Server
Email-
Server
KH X
GIN
Peering Point
Arztpraxis A
ELGA / BRZ
ecard

Angriffs-Schritt 2

„Phishing“

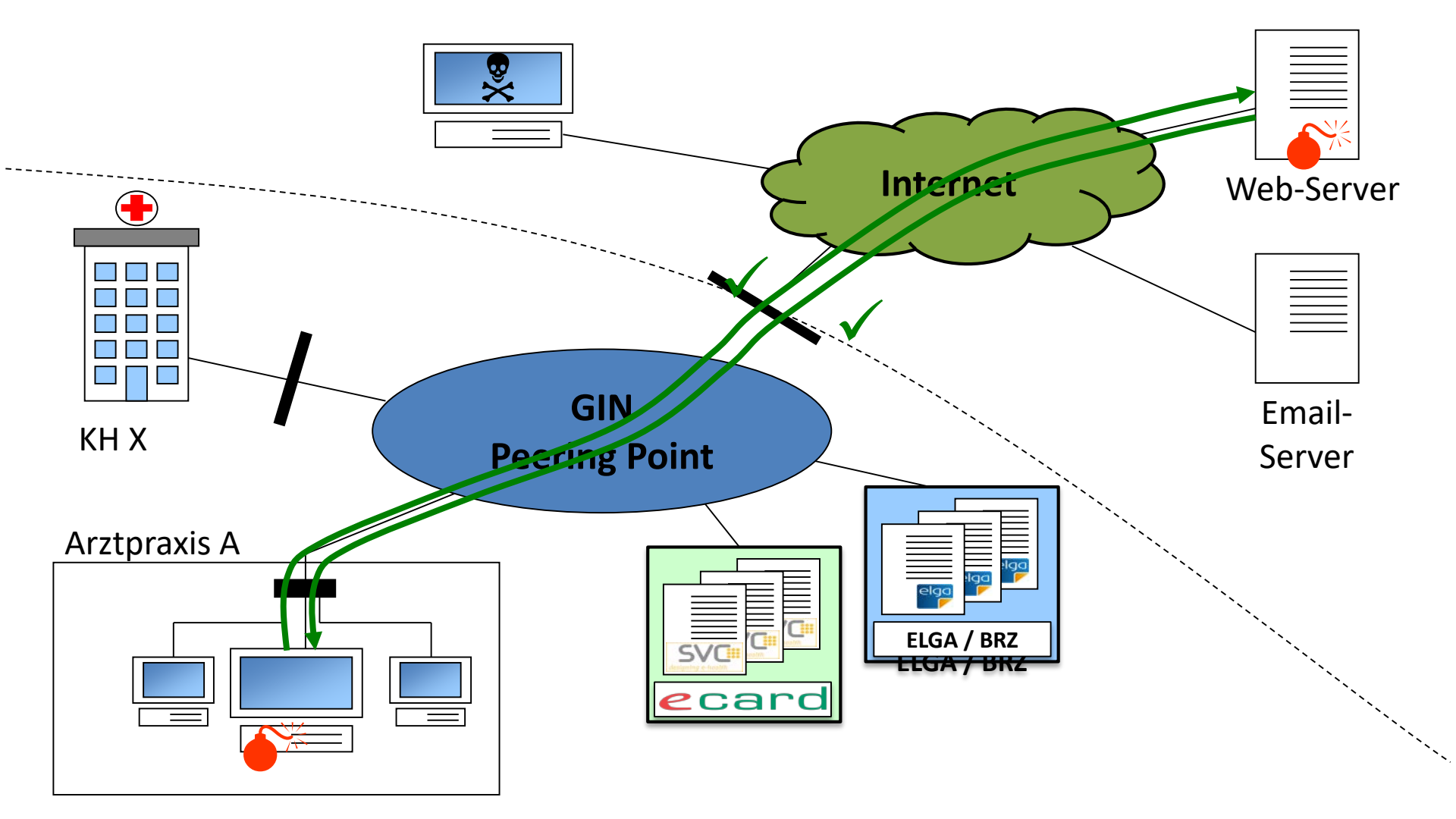
Versenden eines Lock-Emails

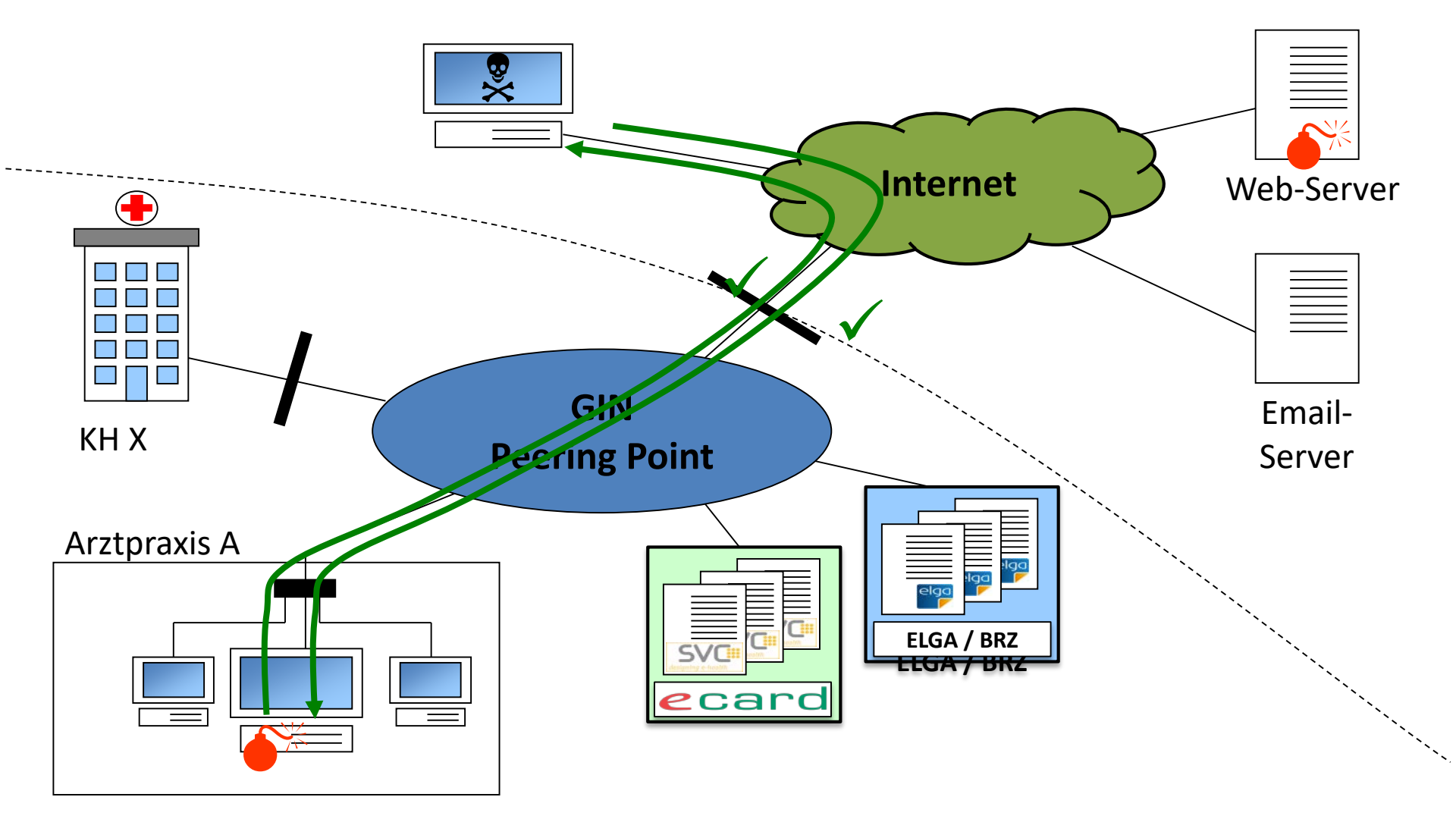

Internet
Web-Server
Email-
Server
KH X
GIN
Peering Point
Arztpraxis A
SVC
ecard
elga
ELGA / BRZ


Internet
Web-Server
Email-
Server
KH X
GIN
Peering Point
Arztpraxis A
ELGA / BRZ
ecard

Angriffs-Schritt 3

Übernehmen des Opfer-Rechners


Internet
Web-Server
Email-
Server
KH X
GIN
Peering Point
Arztpraxis A
ELGA / BRZ
ecard

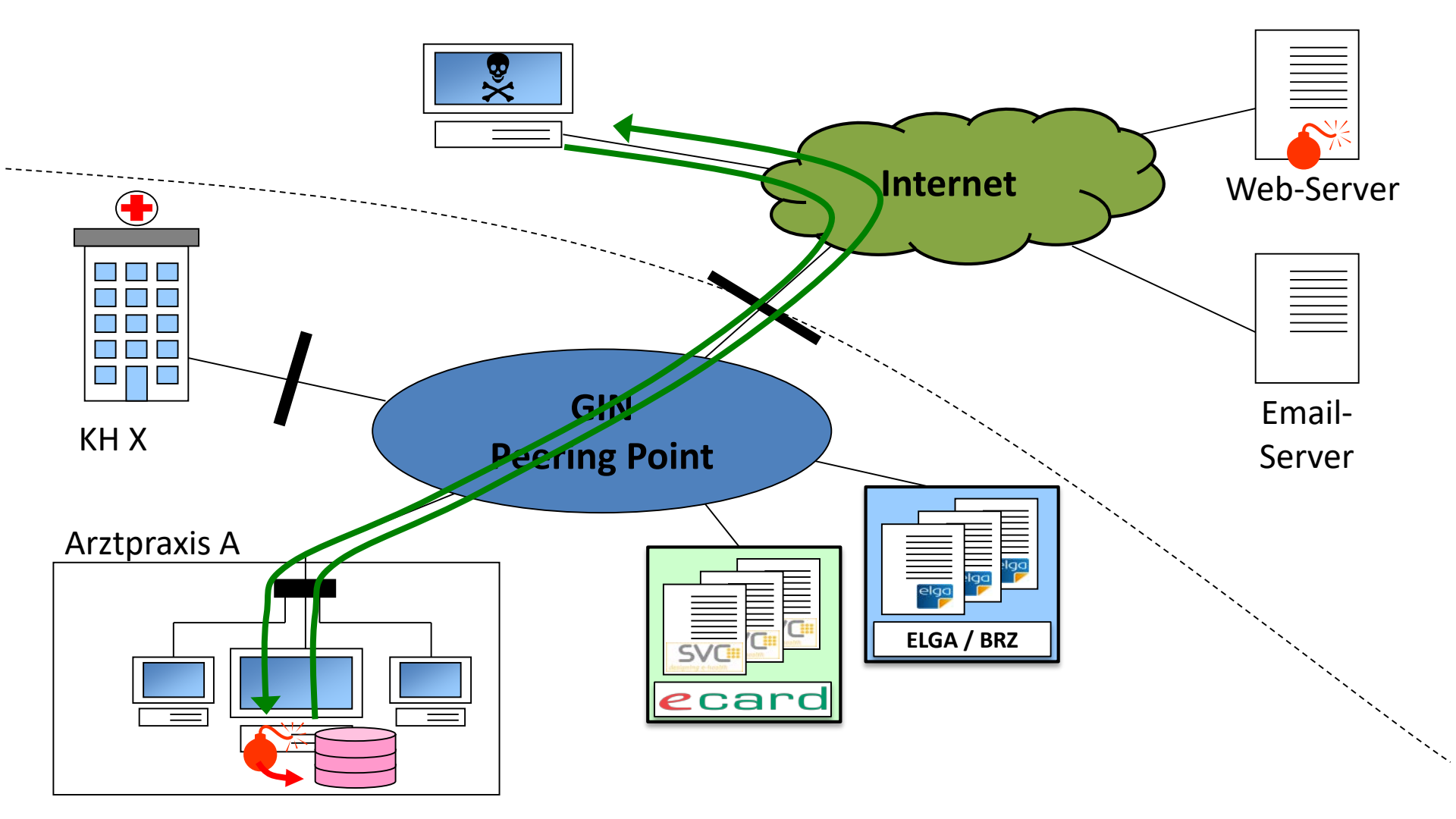

Internet
Web-Server
Email-
Server
KH X
GIN
Peering Point
Arztpraxis A
SVC
ecard
ELGA / BRZ

Was kann Angreifer nun?

- Screenshots
- Webcam / Mikrofon
- Email-Kommunikation abfangen
- Tastatur-Sniffen (eCard-PIN-Code!)

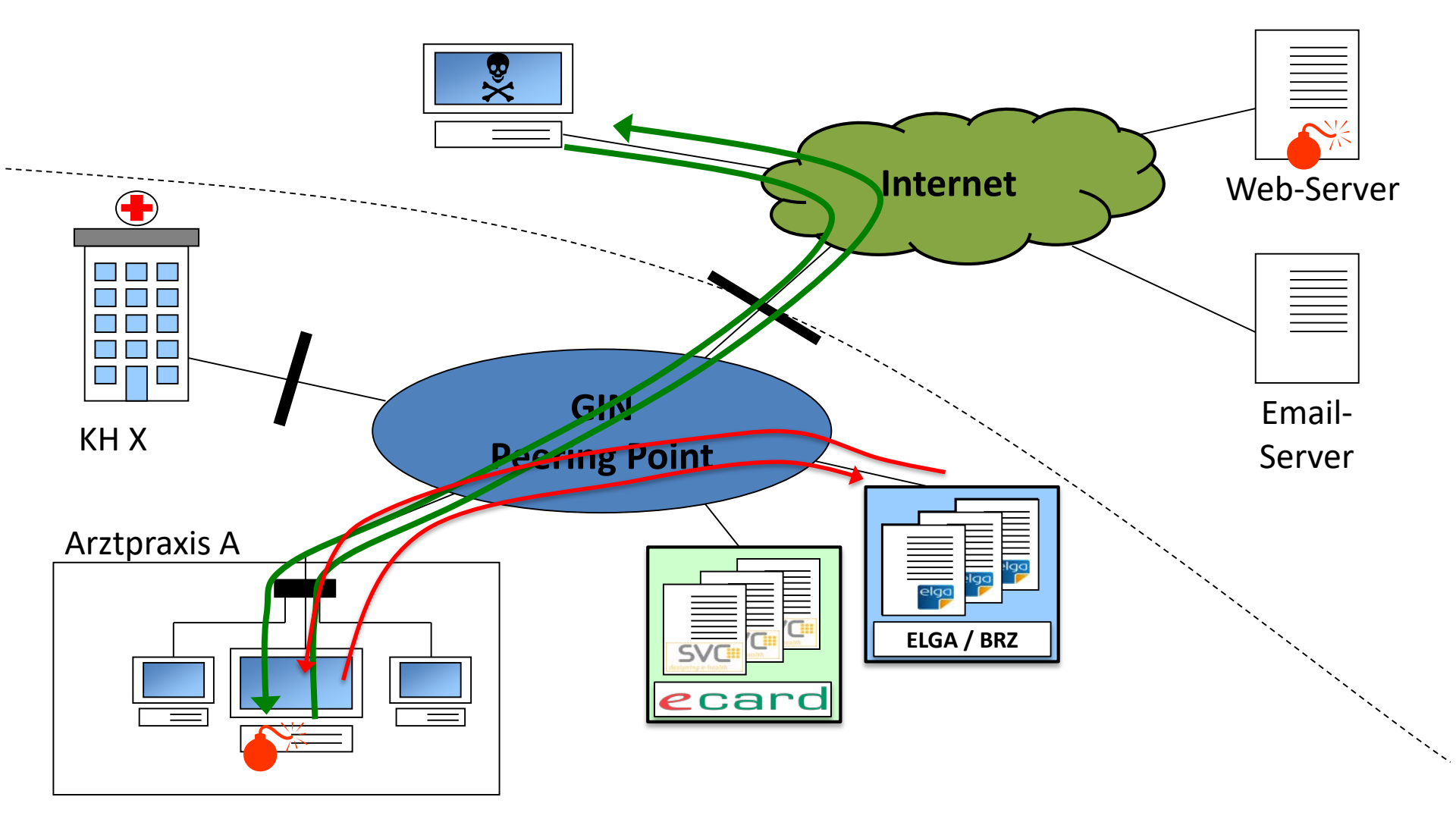
Was kann Angreifer nun?

- die Datenbank des Ordinationsservers kopieren
- sämtliche Festplatten im Ordinationsnetz verschlüsseln (Ransomware)


Internet
Web-Server
KH X
GIN
Peering Point
Email-
Server
Arztpraxis A
SVC
ecard
elga
ELGA / BRZ

Was kann Angreifer noch tun?

- Die Ordinationsrechner für weitere Hacking Aktivitäten und DOS-Angriffe missbrauchen
- auf die ELGA zugreifen und sämtliche ELGA-Daten der freigeschalteten Patienten (Kontaktbestätigung!) nach Außen übertragen


Internet
Web-Server
Email-
Server
KH X
GIN
Peering Point
Arztpraxis A
ELGA / BRZ
ecard

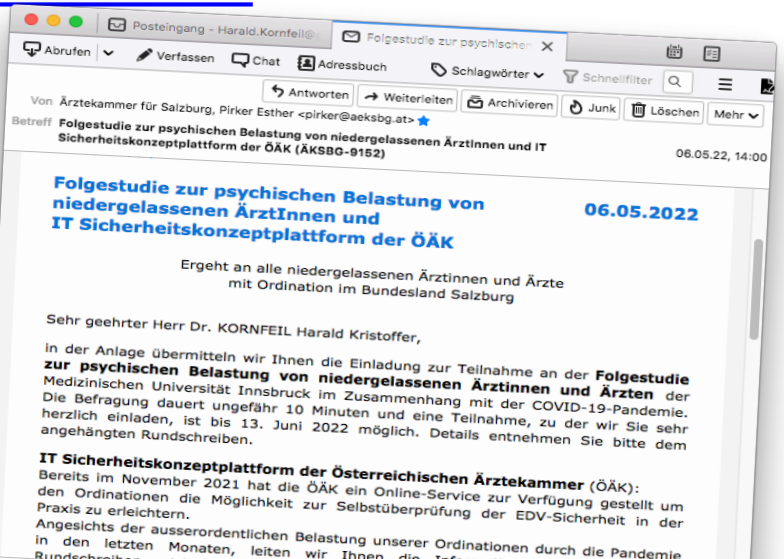
Alles klar?

© 2017 HBO / John Oliver

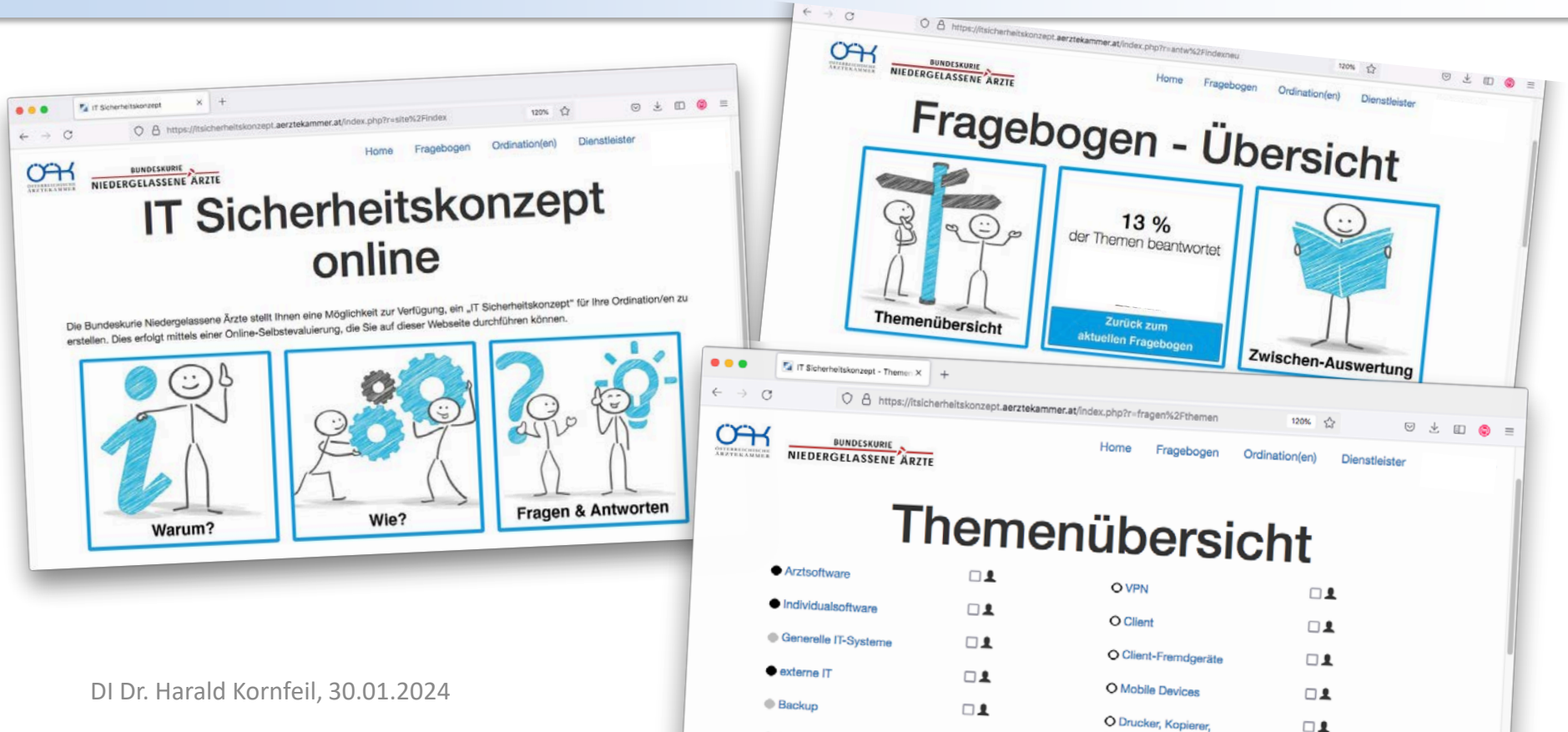
IT-Sicherheitskonzeptplattform

IT-Sicherheitskonzeptplattform der Österreichischen Ärztekammer

https://itsicherheitskonzept.aerztekammer.at



IT-Sicherheitskonzeptplattform



DI Dr. Harald Kornfeil, 30.01.2024

Fragen?

Fragen?

Fragen?

Fragen?

Fragen?

Fragen?

Fragen?

Fragen?

Fragen?

ENDE

Vielen Dank für die Aufmerksamkeit

DI Dr. Harald Kornfeil, 30.01.2024