

**»Sind leider gewachsene  
Strukturen ...«"**

## → **Heinlein Support**

- IT-Consulting und 24/7 Linux-Support mit ~45 Mitarbeitern
- Eigener Betrieb eines ISPs seit 1992
- Täglich tiefe Einblicke in die Herzen der IT aller Unternehmensgrößen

## → **24/7-Notfall-Hotline: 030 / 40 50 5 - 110**

- Spezialisten mit LPIC-2 und LPIC-3
- Für alles rund um Linux & Server & DMZ
- Akutes: Downtimes, Performanceprobleme, Hackereinbrüche, Datenverlust
- Strategisches: Revision, Planung, Beratung, Konfigurationshilfe

## Projekte könnten perfekt laufen ...

- ... wenn nicht immer was dazwischen kommen würde
- optimalerweise Ansatz für ein neues Projekt
- Best-Practices in der Projektplanung
- Best-Practices mit Abstrichen nach Vorstellung mit Chef / größerer Runde
- mindestens ein großes Loch nach Absegnung durch die Führungsetage
- Übernahme von Altlasten bei der Migration wegen Zeitmangel
- weitere (technische) Abstriche bei der Umsetzung der Löcher
- Rücknahme einiger Maßnahmen nach Kundenbeschwerden
- Finally - alte Infrastruktur auf neuen Beinen

## Projekte werden immer wieder aus **Bequemlichkeit** eingegrenzt

- Weil das halt schon immer so war
- Oder die Notwendigkeit nicht gesehen wird
- Viele solcher, wenn auch nur kleiner, Einschränkungen verhindern oft die Nutzung neuer (Sicherheits-) Technologien → DMARC/DANE
- Potenzielle Security issues werden erst genauer geprüft wenn es geknallt hat oder wenn es „das Management auf dem Golf Platz aufschnappt“

## Der Uni Professor und sein Gmail Account

- Alias: CEO mit der Schatten-IT schon im O365
- Impliziert das Mails potenziell auch von dort angenommen werden müssen
  - Und es eben bestimmte Ausnahmen dafür geben muss
  - Zu unspezifische Ausnahmen sind quasi immer ein Sicherheitsrisiko
- Verhindert zuverlässig die Einführung von DMARC (wenn man nicht gleich Google und/oder Microsoft) mit ins SPF übernimmt
- Datenschutz?

## Externe Cloud Services senden im Namen unserer Domain

- Alias: Das Marketing hat mal wieder einen neuen Newsletter Anbieter
- Alias: Fürs Homeoffice brauchen wir ganz schnell diesen Sharing-Dienst
- Mails mit der eigenen Domain kommen immer wieder von anderen Quellen von außen ins interne Netzwerk
- Meistens muss das dann ganz schnell freigeschaltet werden
- Auch ohne weitere Sicherungsmaßnahmen wie DKIM
- Aber: viele Anbieter sind hier in den vergangenen Jahren viel besser geworden

## Studenten fallen ständig auf Phishing Mails rein

- Studenten leiten ihre Mails oft an private Accounts weiter und lesen diese dann auf dem Smartphone
- Phishing Mails lassen sich da gar nicht so gut erkennen
- Sie sind oft sogar recht gut gemacht
- Wenn noch dazu kommt, dass die Nutzung der eigenen Domain von außen nicht eingeschränkt (werden kann) ist, dann gehts ganz schnell

## Wir nehmen erstmal alle Spam Mails an und taggen

- Die Verlustangst bei der E-Mail-Zustellung ist immer noch hoch
- Eine sofortige Ablehnung läßt dem Absender auch sofort eine Bounce Nachricht zukommen
- Die getaggte Spam Mail landet wahrscheinlich automatisch im Junk
- Auch Spam ist ein Teil der IT-Security, aber meist gibt es nur bei Viren die klare Policy diese Mails abzulehnen
- Noch eine Stufe drüber: Wir löschen bestimmte eingehende Mails (Discard) und senden dem EMPFÄNGER eine Benachrichtigung
- <https://www.helein-support.de/vortrag/rechtsfragen-fuer-administratoren-und-unternehmen>



## Verschlüsselungsgateway aber keine Transportverschlüsselung

- Kommunikation zwischen bestimmten Absendern und Empfängern soll zu Erhöhung der Abhörsicherheit via SMIME Zertifikaten verschlüsselt werden
- Mit einem Gateway wie Zertificon oder Cyphermail wird aber gar keine Ende zu Ende Verschlüsselung erreicht, da erst nach dem Versand und schon vor dem Empfang durch den Enduser Ver- oder Entschlüsselt wird
- Es sollte genauso die Transportverschlüsselung forciert werden und abfischen dieser Mails im internen Netzwerk verhindern zu können
- Außerdem sind immer noch Metadaten aus SMIME verschlüsselten Mails extrahierbar, wenn der Transportweg unverschlüsselt bleibt

## SSL aus 2010

- Windows XP Rechner / alter Unix Server wegen einer Uralten, aber wichtigen Software noch im Einsatz
- Deshalb müssen die Mail-Server immer noch SSLv3 sprechen?
- Oder alte Config einfach auf den neuen Server übernommen und damit mögliche neue bessere Verschlüsselungsoptionen ausversehen abgeschaltet?
- Alte Software besser in eine DMZ einsperren und spezielle Gateways bereit stellen
- TLS Optionen immer mal wieder prüfen:
  - <https://ssl-config.mozilla.org/>
- TLS Optionen nicht absolut setzen, sondern unsichere ausschließen
  - !SSLv3, !TLSv1 etc.

## Nehmt euch genug Vorlauf für ein Projekt

- fangt ruhig 1 Jahr vorher an die Alt-Daten zu sichten
- frühzeitig unbequeme Änderungen ins Management tragen
- keine Angst vor neuen Technologien
  - in den meisten Fällen kann doch irgendwie sanft migriert werden

**Soweit, so gut.**

**Gleich sind Sie am Zug:  
Fragen und Diskussionen!**

## **Wir suchen:**

Admins, Consultants, Trainer!

## **Wir bieten:**

Spannende Projekte, Kundenlob, eigenständige Arbeit, keine Überstunden, Teamarbeit

...und natürlich: Linux, Linux, Linux...

**<http://www.heinlein-support.de/jobs>**

# Heinlein Support hilft bei allen Fragen rund um Linux-Server

## HEINLEIN AKADEMIE

Von Profis für Profis: Wir vermitteln die oberen 10% Wissen: geballtes Wissen und umfangreiche Praxiserfahrung.

## HEINLEIN HOSTING

Individuelles Business-Hosting mit perfekter Maintenance durch unsere Profis. Sicherheit und Verfügbarkeit stehen an erster Stelle.

## HEINLEIN CONSULTING

Das Backup für Ihre Linux-Administration: LPIC-2-Profis lösen im CompetenceCall Notfälle, auch in SLAs mit 24/7-Verfügbarkeit.

## HEINLEIN ELEMENTS

Hard- und Software-Appliances und speziell für den Serverbetrieb konzipierte Software rund ums Thema eMail.