BSI Forum

offizielles Organ des BSI
Bundesamt
für Sicherheit in der
Informationstechnik

Messepräsenz

# Das BSI auf der it-sa 2015

***Vom 6. bis 8. Oktober 2015 ist das BSI mit einem Stand auf der IT-Security Messe it-sa in Nürnberg vertreten. Wie in den vorangegangenen Jahren unterstützt das BSI gemeinsam mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM e. V.) die Messe als ideeller Träger.***

Am BSI-Stand in Halle 12, Stand 736 können sich Besucher zu zahlreichen Themen der IT- und Informationssicherheit informieren. Präsentationsschwerpunkte sind in diesem Jahr:

- Allianz für Cyber-Sicherheit
- Cloud-Computing
- IT-Grundschutz
- Sicheres mobiles Arbeiten
- Sicherheitszertifizierung
- Sicherheitsberatung

Im „Auditorium“ in der Halle 12 tragen IT-Sicherheitsexperten des BSI zu folgenden Themen vor:

- Cloud-Computing
  Mittwoch, 7. Oktober 2015, 9:30 Uhr
- Allianz für Cyber-Sicherheit – Cyber-Sicherheits-Umfrage 2015, Ergebnisse und Schlussfolgerungen
  Mittwoch, 7. Oktober 2015, 12:00 Uhr

Ergänzt wird das Vortragsprogramm des BSI durch einen Beitrag zur Zertifizierung von IT-Sicherheitsprodukten im „Forum Blau“:

- Zertifizierung von IT-Sicherheitsprodukten und deren Bedeutung für die Standardisierung
  Donnerstag, 8. Oktober 2015, 9:45 Uhr

Des Weiteren richtet das BSI am Mittwoch, den 7. Oktober 2015 im Messezentrum Saal Paris den 3. IT-Grundschutz-Tag 2015 aus, der insbesondere einen Ausblick über die Weiterentwicklung des IT-Grundschutzes geben wird.



## Inhalt



## Impressum

Redaktion:
Matthias Gärtner (verantwortlich)
E-Mail: matthias.gaertner@bsi.bund.de

Sebastian Bebel
E-Mail: sebastian.bebel@bsi.bund.de

Bundesamt für Sicherheit
in der Informationstechnik (BSI)
Referat Öffentlichkeitsarbeit und Presse
Postfach 20 03 63
53133 Bonn

Hausanschrift:
Godesberger Allee 185–189
53175 Bonn

Telefon: +49 228 999582-0
Telefax: +49 228 999582-5455

Web: www.bsi.bund.de
www.bsi-fuer-buerger.de

Das BSI-Forum, Organ des Bundesamtes für Sicherheit in der Informationstechnik in Bonn, ist Bestandteil der <kes> – Die Zeitschrift für Informations-Sicherheit
23. Jahrgang 2015

IT-Sicherheit 2015–2017:

# Das (Wieder-)Erwachen des Datenschutzes ?

***Im Rahmen des BSI-Kongresses 2015 wurde durch das Referat Informationssicherheit und Digitalisierung des BSI eine Umfrage im Themenfeld IT-Sicherheit durchgeführt. Ziel war es die mittelfristigen Entwicklungen dieses Themenfeldes und seiner Trends zu untersuchen, um daraus einen Erkenntnisgewinn für die eigene Positionierung innerhalb der IT-Sicherheit in den Jahren 2015–2017 abzuleiten.***

*Von Sven Herpig und Jonas Postneek, BSI*

„Es ist nicht unsere Aufgabe, die Zukunft vorauszusagen, sondern auf sie gut vorbereitet zu sein." So mahnte der attische Staatsmann Perikles vor zirka 2500 Jahren, damals bezogen auf die Zukunft Athens. Doch der Satz passt auch, wenn sich heute mit Informationstechnologie beschäftigt wird, sollen doch die Trends nicht um ihrer selbst willen erkannt werden, sondern um besser (lies: sicherer) auf die Zukunft vorbereitet zu sein.

Nicht erst seit den Veröffentlichungen über die digitalen Angriffe der letzten Jahre weiß man, dass auf allen Ebenen größere Anstrengungen für die Sicherung der IT-Systeme unternommen werden müssen. Doch welchen Weg nehmen diese Entwicklungen? In welchem Bereich wird IT-Sicherheit in der nächsten Zeit eine Rolle spielen? Auf was müssen sich Verwaltung, Wirtschaft und Wissenschaft in den nächsten Jahren einstellen? Das BSI hat auf dem 14. IT-Sicherheitskongress die im Folgenden beschriebene Umfrage durchgeführt, um genau diesen Fragen nachzugehen.

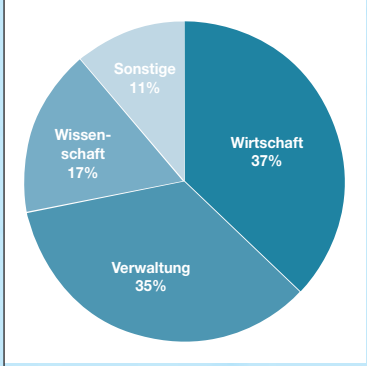


*Abbildung 1: Hintergrund der Umfrageteilnehmer*

## Forschungsdesign und Vorgehen

Das Forschungsdesign der Umfrage wurde möglichst stringent und einfach gehalten. Zuerst wurden mittels Team-Brainstorming des durchführenden BSI-Referats 24 Themen ermittelt, die in den nächsten drei Jahren (2015–2017) mit Bezug auf die IT-Sicherheit wichtig werden könnten. Der relativ kurze Zeitraum wurde wegen der starken Veränderungen und Umwälzungen, denen die IT-Landschaft unterworfen ist, gewählt. Die ermittelten Themen wurden in aktueller Fachliteratur und mittels einer Medienanalyse auf ihre Tauglichkeit als „Emerging Issue" hin geprüft.

Es ergaben sich 15 Themen, die Eingang in den Fragebogen fanden: Big Data, Car-to-X, Cloud-Computing, Datenschutz, digitale Souveränität, E-Government, E-Health, Industrie 4.0, Mobile Payment, politisch motivierte Cyberangriffe, Smart City, Smart Grid, Smart Home, soziale Medien und Wearables.

Im Fragebogen wurde auf einer Skala von eins bis sechs nach der IT-Sicherheitsrelevanz der alphabetisch sortierten Themen für den genannten Zeitraum gefragt; es war auch möglich, keine Angabe zu machen. Zusätzlich bestand die Möglichkeit, ein eigenes – noch nicht in der Umfrage genanntes – Thema zu benennen. Nach der Rückgabe wurden die Fragebögen einer qualitativen und quantitativen Auswertung unterzogen. Neben der Gesamtauswertung fanden eine, nach der Herkunft der Teilnehmer getrennte, sektorale Auswertung sowie eine Korrelationsanalyse statt.

## Gesamtergebnis

Der Fragebogen wurde an 500 Teilnehmer des BSI-Kongresses ausgeteilt. Es ergab sich eine Rücklaufquote von 17,8 %, das entspricht 89 Fragebögen (100 % gültig).

Die Top-6-Ergebnisse, also jene mit dem durchschnittlich höchsten Bewertungsergebnis im Bezug auf ihre IT-Sicherheitsrelevanz bis 2017 sind (vgl. Abb. 2):

1. Datenschutz
2. Cloud-Computing
3. Politisch motivierte Cyberangriffe
4. Digitale Souveränität
5. Big Data
6. Industrie 4.0

Die Ergebnisse zeigen, dass sich die sechs Themen mit der höchsten Relevanz deutlich vom Rest absetzen: Das Delta der durchschnittlichen Bewertungen zwischen Platz 1 „Datenschutz“ und Platz 6 „Industrie 4.0“ beträgt gut 10 %, während das Delta zwischen Platz 6 und Platz 7 „Car-to-X“ 6,57 % beträgt.

## Korrelationen

Eine Korrelation der Top-6-Themen über die höchste Bewertungsstufe („6 – sehr relevant“) mit jeweils allen anderen Themen zeichnet folgendes Bild: Generell korrelieren die Top-6-Themen stark untereinander (siehe Abb. 3) – mit einer Ausnahme: Industrie 4.0. Bei den restlichen fünf Top-6-Themen findet sich kein Thema, welches über die höchste Bewertungsstufe bei den jeweiligen Top-3-Korrelationen mit Industrie 4.0 korreliert.

Industrie 4.0 korreliert allerdings selbst wieder stark mit den Top-6-Themen unter anderem mit Cloud-Computing, Datenschutz und politisch motivierten Cyberangriffen. Dies bedeutet, dass die Gruppe der Personen, welche die Top-5-Themen als wichtig erachtet haben, homogen ist, sich aber gleichzeitig auch von Industrie 4.0 abgrenzt.

Darüber hinaus ist bemerkenswert, dass das auf Platz 7 gelegene Thema Car-to-X zwei Mal in den Top-3-Korrelationen der Top-6-Themen auftaucht (bei Cloud und Industrie 4.0). Es liegt nahe, dass Car-to-X als Thema inhaltlich eher bei der gleichen homogenen Personengruppe verortet ist wie das Thema Industrie 4.0.

## Top-6 nach Teilnehmergruppen

### Gruppe Wirtschaft

1. Datenschutz
2. Politisch motivierte Cyberangriffe
3. Digitale Souveränität
4. Cloud-Computing
5. Car-to-X
6. Big Data

Bei der Gruppe der Wirtschaft fällt auf, dass Car-to-X den Sprung in die Top-6-Themen geschafft hat und damit Industrie 4.0 verdrängt (Platz 10). Weiterhin ist die relativ hohe Einstufung von Wearables (Platz 9) im Vergleich zur Gesamtliste (Platz 15) interessant.

### Gruppe Verwaltung

1. Datenschutz
2. Cloud-Computing
3. Politisch motivierte Cyberangriffe
4. Big Data
5. Digitale Souveränität
6. Industrie 4.0

Auffälligkeiten bei den Ergebnissen in der Gruppe Verwaltung zeigen sich in der relativ hohen Einstufung von sozialen Medien (Platz 9) im Vergleich zur Gesamtliste (Platz 12) und den anderen Zielgruppen (Plätze 13, 14 und 15).

### Gruppe Wissenschaft

1. Datenschutz
2. Cloud-Computing
3. Politisch motivierte Cyberangriffe
4. Big Data
5. Industrie 4.0
6. Digitale Souveränität

Bei den Top-6-Themen aus der Gruppe Wissenschaft gibt es keine besonderen Auffälligkeiten mit Blick auf das Gesamtergebnis.

### Gruppen Sonstige und keine Angabe

1. Industrie 4.0
2. Politisch motivierte Cyberangriffe, Cloud-Computing und Datenschutz

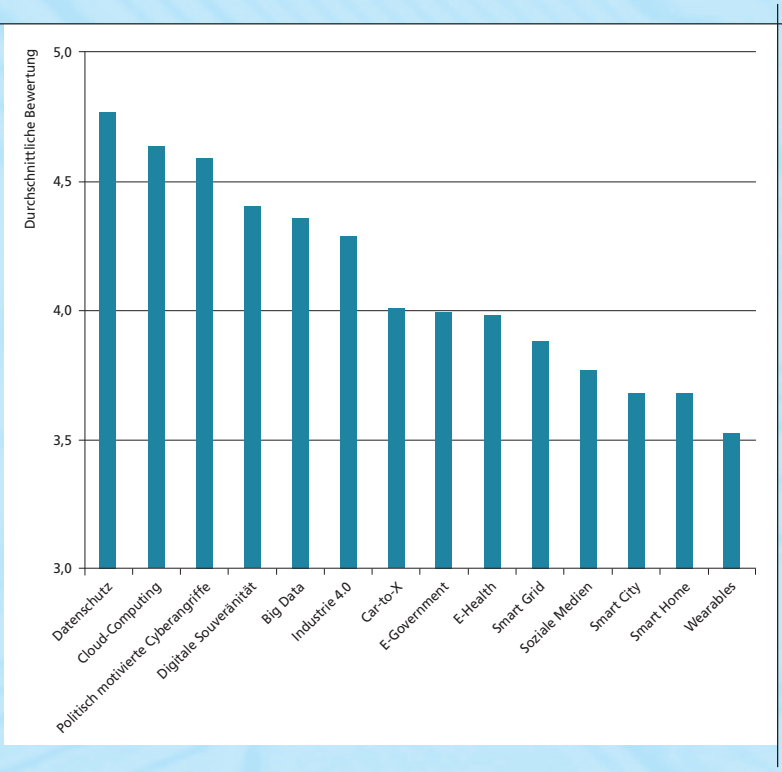


*Abbildung 2: Gesamtergebnis*

5. Digitale Souveränität, E-Health und Smart Grid

Bei diesen Gruppen ist die hohe Bewertung von Industrie 4.0 (Platz 1) im Vergleich zu den Gesamtergebnissen (Platz 6) auffällig, genauso wie die niedrige Einstufung von Big Data (Platz 8 statt Platz 5).

## Ergänzende Themen

In einem Textfeld des Fragebogens konnten Ergänzungen zu den bereits im Fragebogen erwähnten Themen genannt werden. Dies wurde nur marginal genutzt, darüber hinaus wurden meist keine Einzelthemen, sondern Themenkomplexe sowie bereits abgefragte Themen unter anderer Bezeichnung genannt. Genannt wurden mobile IT-Lösungen, das IT-Sicherheitsbewusstsein der Bürger, das Internet der Dinge sowie sichere Hardware und Verschlüsselung.

## IT-Trends in anderen Studien

Zur Reflexion unserer Ergebnisse wurden zwei IT-Trendanalysen mit Bezug auf einen, der eigenen Umfrage ähnlichen, Untersuchungszeitraum herangezogen – zum einen den eco-Report „IT-Sicherheit 2015“ und zum anderen die Gartner-Studie „Top 10 Strategic Technology Trends for 2015“. Es wurde untersucht, inwiefern die Platzierung der Top-6-Themen in der durchgeführten Studie mit denen von eco und Gartner korrespondieren.


*Abbildung 3: Korrelationen in den Top-6-Themen*

Für ihren Report wurden vom eco – Verband der deutschen Internetwirtschaft e. V. 280 IT-Sicherheitsexperten bezüglich der Relevanz von IT-Sicherheitsthemen für das Jahr 2015 befragt. Die dort gefundenen Top 6 IT-Sicherheitstrends für das Jahr 2015 sind:

1. Datenschutz
2. Mitarbeiter-Sensibilisierung
3. Verschlüsselung und Mobile-Device-Security
4. über das Internet verbreitete Schadsoftware
5. Cloud-Security und Notfallplanung sowie
6. Zero-Day-Attacken

Vergleicht man diese Ergebnisse mit jenen der von den Autoren durchgeführten Befragung, fällt sofort auf, dass Datenschutz in beiden Arbeiten den Spitzenplatz einnimmt. Ebenfalls schafft es das Thema Cloud-Computing bei beiden Arbeiten in die Top 6 (Platz 2 in der vorliegenden Studie und Platz 5 in der eco-Studie). Außerhalb der Top-6-Themen landet in beiden Untersuchungen das Thema „soziale Medien“ übereinstimmend und abgeschlagen auf Platz 12.

In der Gartner-Studie belegen Computing Everywhere (1), Internet of Things (2), 3D-Printing (3), Advanced, Pervasive and Invisible Analytics (4), Context-Rich Systems (5) und Smart Machines (6) die ersten sechs Plätze. Ein Vergleich zwischen der Gartner-Studie und der vorliegenden Auswertung kann nicht als vollständig valide gelten. Denn anders als unsere Umfrage oder jene von eco, handelt es sich bei der Gartner-Studie um eine breit angelegte Analyse, mit einem großen Datenpool.

Gleichwohl ergeben sich zwischen den Arbeiten Überschneidungen: Dies ist sowohl bei Industrie 4.0 als auch bei Big Data der Fall. Auffällig ist, dass die Gartner-Studie die Smart-X- und Internet-of-Things-

Trends als sehr relevant wertet, während sie in der, dem Artikel zugrunde liegenden, Umfrage eher schwach wegkommen. Es besteht die Annahme, dass dies aufgrund der Wirtschaftsaffinität der Gartner-Studie der Fall ist, da es sich bei diesen Bereichen eher um für Wirtschaft potenziell interessante Bereiche handelt als zum Beispiel bei den Themen Datenschutz oder politisch motivierte Cyberangriffe.

## Bewertung der Umfrage

Die auf dem BSI-Kongress 2015 durchgeführte Umfrage ergab für die nächsten zweieinhalb Jahre keine unerwarteten Themen. Datenschutz, Cloud-Computing, politisch motivierte Cyberangriffe, digitale Souveränität, Big Data und Industrie 4.0 sind als Trends in der „IT-Sicherheitsszene“ bekannt und werden von ihr bereits ausführlich diskutiert. Dies wird durch die beiden untersuchten Studien noch einmal bestätigt und durch die enge Korrelation der Top-6-Themen unserer Studie untereinander nahegelegt.

Das BSI als zivile IT-Sicherheitsbehörde des Bundes befasst sich bereits heute mit den ermittelten Trends. So wird beispielsweise im Bereich des (technischen) Datenschutzes gearbeitet: Dabei stehen so vielfältige Themen wie die Datensicherheit, die Schnittstelle von IT-Sicherheit und Datenschutz oder eID-Anwendungen auf der Agenda des Hauses.

Hierbei kann ein wirksames Arbeiten nur interdisziplinär erfolgen. So bedarf ein wirksamer Datenschutz im digitalen Zeitalter sowohl technischer Komponenten (z. B. Datensicherheit) als auch rechtlicher Komponenten (z. B. Verfahren bei der Nutzung der Daten). Um hier erfolgreich zu sein, bedarf es der Zusammenarbeit verschiedener Stellen innerhalb und außerhalb des BSI. Ein solcher interdisziplinärer Ansatz erfolgt nicht nur beim Datenschutz, sondern auch bei anderen Thermen (z. B. Big Data und Cloud-Computing). Das BSI kann die Herausforderungen in der IT-Sicherheit nur gemeinsam mit seinen Partnern in Wirtschaft, Verwaltung und Wissenschaft lösen.

Mit dem Thema Cloud-Computing befasst sich das BSI seit einiger Zeit sehr intensiv. So wurde das Eckpunktepapier „Sicherheitsempfehlungen für Cloud-Computing-Anbieter“ bereits 2011 Cloud-Dienstleistern mit Mindestsicherheitsanforderungen zur Verfügung gestellt. Über technische und organisatorische Aspekte hinaus wurden Compliance-Anforderungen definiert und der Zugriff auf die Daten durch Dritte thematisiert. So konnten auch Cloud-Nutzer von dem Eckpunktepapier profitieren: Sie fanden Kriterien vor, die sie als Maßstab an Cloud-Anbieter anlegen konnten.

Der bewährte IT-Grundschutz als das Standardwerk für die Informationssicherheit wurde bereits um viele Cloud-spezifische Aspekte erweitert, sodass eine Zertifizierung von Cloud-Anbietern nach IT-Grundschutz möglich geworden ist. Die vom BSI 2014 herausgegebene Broschüre „Sichere Nutzung von Cloud-Diensten“ zeigt dem interessierten Nutzer Schritt für Schritt einen strukturierten Weg zur sicheren Cloud. Mit dem ebenfalls 2014 vorgestellten Sicherheitsprofil „Software as a Service“ (SaaS), wurde vom BSI eine umfassende Risikodarstellung vorgelegt, aus der ein prüfbarer Anforderungskatalog für Cloud-Dienstleister erstellt werden konnte. Das BSI adressiert Sicherheit im Cloud-Computing auch für vom Bund selbst betriebene Cloud-Infrastrukturen, zum Beispiel bei der geplanten „Bundescloud“.

Bei Cyberangriffen jedweder Art unterstützt das BSI die Bundesverwaltung vielfältig – unter anderem durch Sicherheitsberatungen und operative Netzabwehr bei den an den Informationsverbund Berlin Bonn (IVBB) angeschlossenen Behörden. Weiterhin betreibt es das IT-Lagezentrum des Bundes sowie das Computer-Emergency-Response-Team des Bundes (CERT-Bund).

Das BSI trägt durch die Prüfung und Zertifizierung von IT-Produkten zur digitalen Souveränität in Deutschland bei. Darüber hinaus kooperiert die Behörde mit Akteuren aus Wirtschaft, Verwaltung, Wissenschaft und Gesellschaft in den entsprechenden Bereichen der IT-Sicherheitslandschaft.

Im Bereich Industrie 4.0 engagiert sich das BSI in der Plattform „Industrie 4.0“ des Bundesministeriums für Wirtschaft und Energie. Ziel ist es IT-Sicherheitsaspekte direkt beim Design von Industrie-4.0-Lösungen zu berücksichtigen. Das BSI bringt hierzu seine Expertise in die Plattform ein. Darüber hinaus werden mittels des ICS-Security-Kompendiums und den Cybersicherheitsempfehlungen der Allianz für Cybersicherheit die Sensibilisierung von Betreibern und Herstellern von Industrie- und Automationsanlagen / Automationskomponenten im Bereich Cybersicherheit gefördert.

Auch in den von den Antwortgebern zusätzlich genannten Bereichen ist das BSI aktiv: So treibt das Haus zum Beispiel die Förderung des IT-Sicherheitsbewusstseins mit dem Angebot „BSI-für-Bürger“ voran. Das Angebot umfasst eine Internetplattform mit allgemeinen Informationen zum sicheren Umgang mit dem Internet sowie ein „Bürger-CERT“ mit Newsletter und aktuellen, auf die Privatanwender abgestimmten Warnmeldungen.

## Fazit

Die in der Gesellschaft vorherrschende, niedrige sicherheitssensitive Bewertung von derzeit schnell fort-

schreitenden Technologiefeldern wie E-Health, Mobile Payment oder Smart Cities stellt ein latentes Problem der IT-Sicherheit da. Auch wenn eine A-priori-Einbindung von Sicherheitsaspekten (Security und Privacy by Design) bei Entwicklungen im IT-Bereich immer problematisch erscheint – z. B. aufgrund des „Time to Market" – ist sie dennoch unerlässlich.

Die Durchdringung aller Bereiche der Gesellschaft mit Informations- und Kommunikationstechnologie kann nur dann ein Gewinn für alle sein, wenn sie nicht gleichzeitig auch eine Durchsetzung der Gesellschaft mit (IT-)Verwundbarkeiten darstellt. Gerade bei den hier als nicht so hoch bewerteten Trends ist es erforderlich, dass die entsprechenden Akteure (wie z. B. Verbände und Sicherheitsexperten) zusammenkommen, um das „IT-Sicherheitspferd vor den Karren zu spannen", solange es noch möglich ist.

Es handelt sich um eine Herausforderung, die nur mit einem gesamtgesellschaftlichen Ansatz beantwortet werden kann, ja vielleicht sogar mit einer gesamtgesellschaftlichen Kraftanstrengung – einem Zusammenspiel aus Politik, Wirtschaft, Wissenschaft und Gesellschaft. Nur dann können wir, Perikles Mahnung vom Anfang folgend, gut auf die zukünftigen Herausforderungen in der IT-Sicherheit vorbereitet sein.

Die Autoren bedanken sich bei allen Teilnehmern der Trendstudie. Wir freuen uns auf ein Wiedersehen mit alten und neuen IT-Sicherheitstrends beim 15. IT-Sicherheitskongress. ■

# hardFIRE

## Ein Firewall-Konzept auf FPGA-Basis

***Das stark wachsende Datenaufkommen zwingt Firewall-Hersteller zu völlig neuen Konzepten bei der Filtertechnologie. Im Forschungsprojekt hardFIRE soll die Nutzbarkeit von rekonfigurierbaren Logikbausteinen für diese Aufgabe anhand einer konkreten Implementierung untersucht werden.***

*Von Andreas Fießler, genua GmbH – Gewinner des Best-Student-Awards beim 14. Deutschen IT-Sicherheitskongress*

Während die ersten Firewalls lediglich statische Paketfilter auf Basis von Netzwerkadressen, Transportschicht-Ports und -protokoll implementierten, ist dies heute bei Weitem nicht ausreichend, um ein Netzwerk vor den simpelsten Angriffen zum Beispiel auf Basis von IP-Spoofing zu schützen.

Daher verwenden moderne Firewall-Systeme eine Reihe von weiteren Techniken, welche von zustandshaltender Paketfilterung über Deep-Packet-Inspection (DPI) bis hin zu spezialisierter Applikationskontrolle mithilfe von Application-Level-Gateways (ALG) reichen. Weitverbreitete Systeme sind beispielsweise iptables und pf sowie die Intrusion-Detection-Systeme (IDS) Snort und Bro.

Die Bandbreite der zugrunde liegenden Hardware-Plattformen reicht hierbei von kleinen Heimroutern bis hin zu leistungsfähigen Serversystemen. Jedes eingehende Netzwerkpaket muss hier über Busse, Speicher und verschiedene Betriebssystemkomponenten verarbeitet und sequenziell mit einem mitunter sehr großen Regelsatz verglichen beziehungsweise die zugehörige Netzwerkverbindung in einem Verbindungsspeicher nachgeschlagen werden.

Bei einer Übertragungsgeschwindigkeit von beispielsweise 100 Gbit/s bleiben dem System hier im Extremfall fünf Nanosekunden pro Paket (64 Byte) für all diese Operationen. Aktuelle Ergebnisse aus der Forschung zeigen, dass selbst schnelle softwarebasierte Paketklassifikationssysteme wie Open vSwitch auch unter guten Bedingungen kaum Datendurchsätze von 10 Gbit/s erreichen.

Den Performance-Limitierungen für Softwarelösungen kann mit verschiedenen Arten von Hardwarebeschleunigung begegnet werden: In höheren Geschwindigkeitsbereichen kommen spezielle Hardware-Firewalls zum Einsatz, die oftmals auf einem dedizierten, anwendungsspezifischen Schaltkreis (Application-Specific Integrated Circuit, ASIC) basieren. Besonders die in Hardware mögliche hochgradige Parallelisierung, wie sie zumeist in Assoziativspeichern (Ternary Content-Addressable Memories, TCAMs) genutzt wird, sorgt dabei für den benötigten Performancegewinn.

ASICs sind in der Entwicklung allerdings sehr komplex und benötigen lange Entwicklungszyklen. Darüber hinaus bieten TCAMs vergleichsweise sehr wenig Speicherplatz und sind sowohl teuer als auch energieineffizient. Ein weiterer großer Nachteil von kommerzieller, dedizierter Hardware ist, dass die verwendeten Komponenten nicht einsehbar sind und somit potenziell Hintertüren enthalten können. Filterungsschaltkreise auf Field-Programmable Gate-Arrays (FPGAs) zu implementieren, ist eine Möglichkeit, diese Nachteile zu vermeiden.

Die existierenden Ansätze zeigen bereits vielversprechende Ergebnisse. Im Forschungsprojekt soll darauf aufbauend zum einen untersucht werden, wie sich das Parallelisierungspotenzial auf dem FPGA optimal ausnutzen lässt. Zum anderen ist der Performancegewinn durch die Spezialisierung der auf dem FGPA implementierten Schaltung gegenüber einer universellen Auslegung von Interesse.

## *Vertrauenswürdige FPGA-Entwicklung*

Aktuelle Untersuchungen und Enthüllungen bestätigen sowohl die Möglichkeit als auch die Durchführung von Angriffen über Hardwarekomponenten. Beispielsweise können durch Kill-Switches Hardwarekomponenten irreversibel deaktiviert oder mit versteckten Schnittstellen unberechtigt geheime Informationen ausgelesen werden. Abbildung 1 zeigt einen exemplarischen Fall, in dem eine einfache Netzwerkkarte – vom Betriebssystem unbemerkbar – Speicherinhalte mit sensitiven Informationen ausliest. Die Daten werden anschließend von der bösartigen Netzwerkkarte eigenständig in einem unauffälligen Paket versteckt und an den Angreifer gesendet. Ein solcher Angriff ist durch den etablierten Speicherdirektzugriff (Direct Memory-Access, DMA) in nahezu jedem modernen Rechnersystem möglich.

Als Gegenmaßnahme können relevante Teile der Hardwarekomponenten selbst entworfen und implementiert werden – beispielsweise durch Eigenentwicklung auf Basis von FPGAs. Dies gewährleistet eine zertifizierbare Funktionalität auf dieser Ebene.

Dennoch bergen beispielsweise geschlossene, vorgefertigte Funktionsblöcke (so genannte IP-Cores), welche verbreitet zur Reduktion des Entwicklungsaufwands eingesetzt werden, vergleichbare Risiken wie integrierte Schaltkreise. Im Vorfeld des Forschungsprojekts wurden hierzu bereits verschiedene Möglichkeiten erarbeitet, um größtmögliche Sicherheit bei vertretbarem Mehraufwand in der Entwicklung zu erreichen. Ziel ist dabei, IP-Cores mit unbekanntem Vertrauensstatus weiterhin verwenden zu können.

Ein relativ einfach umsetzbares Verfahren ist die Verschlüsselung der im IP-Core verarbeiteten Daten (Scrambling). In vielen Fällen benötigt ein IP-Core zur Verarbeitung nur einen sehr kleinen Teil der Metadaten, beispielsweise Beginn und Ende eines Datenpakets. Bei einer effektiven Verschlüsselung der restlichen Daten können sowohl das Auslösen von Hintertüren in IP-Cores durch spezielle Sequenzen als auch der beschriebene DMA-Angriff verhindert werden, da durch die Verschlüsselung Auslösesequenzen nicht erkennbar sind, beziehungsweise ungültige Daten entstehen.

Dieser Ansatz deckt allerdings nur einen Teil möglicher Angriffsvektoren in IP-Cores ab. Werden auf einem FPGA sensitive Daten (zum Beispiel Schlüsselmaterial) verarbeitet, besteht die Möglichkeit, dass ein IP-Core für Unbefugte direkt neue Zugriffswege auf diese Daten erlaubt – beispielsweise durch Seitenkanäle oder sogar direkte Schnittstellen. All diese Gefahren müssen in einer sicheren Implementierung bedacht werden.

### Verbleibende Angriffsvektoren

Im Rahmen der konzeptionellen Arbeiten konnten weitere Risikofaktoren identifiziert werden: Die Design-Tools für FPGAs könnten an vielen Stellen die Funktion der erzeugten Hardware manipulieren. Vergleichbar hiermit ist ein bösartiger Compiler, der Software unbemerkt mit Hintertüren oder Schwachstellen versieht.

Die Fertigung von ICs wird oft an externe Hersteller ausgelagert – auch hier besteht ein Risiko nachträglicher Modifikationen. Zudem können Fälschungen der entsprechenden Schaltkreise in den Produktionszyklus gelangen. Gleichermaßen betrifft dies auch die neben dem eigentlichen FPGA verbauten Komponenten eines Systems.

Ein Angreifer kann versuchen, unbemerkt eine eigene Konfiguration (Bitfile) in den FPGA einzu-

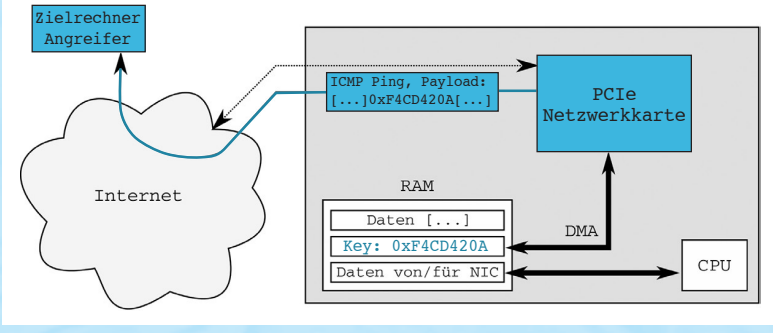


*Abbildung 1: Angriffsszenario mit einer präparierten Netzwerkkarte per DMA.*

spielen. Am Markt etablierte FPGAs bieten hiergegen zwar Schutzmechanismen in Form von verschlüsselten Updates – diese zeigten in der Praxis allerdings bereits Schwachstellen.

Die ersten beiden Punkte erfordern auf Seite des Angreifers sehr detailliertes A-Priori-Wissen über den speziellen Anwendungsfall. Da sowohl Design-Tools als auch FPGAs für ein breites Spektrum an Aufgaben konzipiert werden, kann das Risiko für solche Angriffe als gering eingestuft werden.

## Konzept hardFIRE

Das Ziel von hardFIRE [1] ist, neue Wege aus den im Bereich der Hochleistungs-Firewalls bestehenden Problemen aufzuzeigen und dabei eine Alternative sowohl zu reinen Softwarelösungen als auch zur aufwändigen ASIC-Entwicklung zu bieten. Hierfür wird ein speziell entwickelter Workflow eingesetzt: Die hardFIRE-Toolchain liest einen vom Systemadministrator vorgegebenen Regelsatz ein und erzeugt daraus, wie in Abbildung 2 veranschaulicht, einen spezialisierten, regelsatzspezifischen Schaltkreis. Dieser wird zunächst in der Hardwarebeschreibungssprache VHDL generiert, aus der dann wiederum eine FPGA-Konfiguration synthetisiert werden kann.

Der FPGA wird so als Spezialprozessor genutzt, der nicht nur an die generelle Aufgabe („Firewalling"), sondern darüber hinaus an die spezifische Probleminstanz, also den konkreten Regelsatz, angepasst ist. Der genutzte Schaltkreis kann damit sehr detailliert auf den Regelsatz und damit den konkreten Einsatzort und -zweck optimiert werden. Einzelne Filterkriterien, beispielsweise Adressmasken oder Portbereiche, müssen bei der Paketverarbeitung nicht jeweils aus einem Regelspeicher gelesen, sondern können unmittelbar in die Verarbeitungslogik integriert werden.

Die statische Rekonfiguration des FPGA bei umfangreichen Regelsatzänderungen wird ergänzt um Möglichkeiten, dynamisch punktuelle Konfigurationsaktualisierungen ohne eine vollständige, zeitaufwändige Neusynthese vorzunehmen. Der zunächst vorhandene, bauartbedingte Nachteil von FPGAs gegenüber ASICs – ein identischer Schaltkreis arbeitet auf einem FPGA deutlich langsamer als auf einem ASIC – kann durch die regelsatzspezifische Hardware-Generierung kompensiert werden: Die regelsatzspezifische, in hardFIRE erzeugte Schaltung ist deutlich spezialisierter, da sie nur die für die jeweilige Aufgabe unbedingt notwendige Logik enthält. Deshalb ist sie wesentlich kleiner als eine generische ASIC-Lösung mit vergleichbarer Verarbeitungsparallelität.

Die Kompaktheit der auf dem FPGA zu konfigurierenden Logik erhöht die Performance beträchtlich. Somit wird eine sowohl flexible als auch hoch leistungsfähige Firewall-Lösung erreicht. Die Generierung der Hardwarebeschreibung ist dabei integraler und vollständig automatisierter Bestandteil der Toolchain – der Administrator benötigt daher keine speziellen Hardware-Kenntnisse, um hardFIRE einzusetzen.

Die prinzipielle Anwendbarkeit des geschilderten Wegs wurde in Vorarbeiten bereits für zustandslose Paketfilter unter Beweis gestellt. Im hardFIRE-Projekt wird nun, darauf aufbauend, eine vollständige Firewall-Lösung entstehen. Diese wird auch komplexere Funktionalität, wie

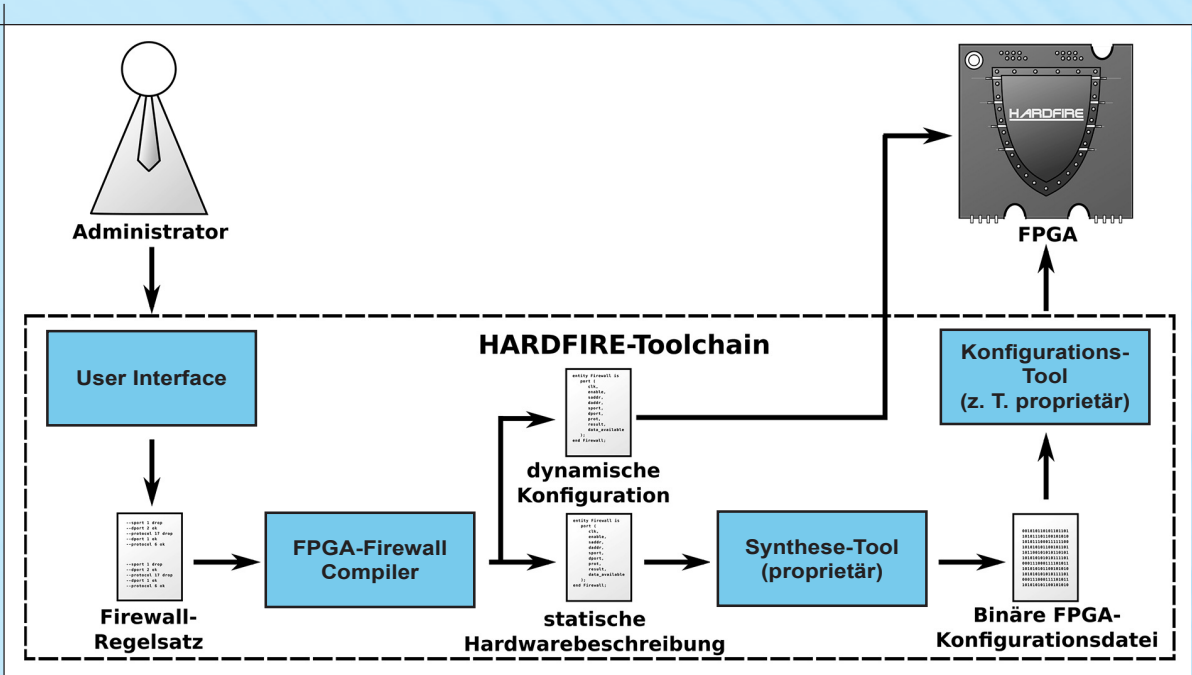


*Abbildung 2: Workflow der hardFIRE-Toolchain*

beispielsweise Connection-Tracking, bieten und somit die Grundlage für einen Einsatz in Produktivumgebungen legen. Abbildung 3 veranschaulicht die Bestandteile und den internen Datenfluss in der hardFIRE-Verarbeitungslogik.

## Sicherheitsaspekte

Neben den Aspekten der Hardware-Sicherheit müssen weitere Details beachtet werden, um eine sichere Konfiguration zu gewährleisten. Ausschlaggebender Unterschied ist die Rolle des Firewall-Herstellers: Dieser stellt bei klassischen Firewalls das System und generische Software beziehungsweise Firmware-Updates bereit. Bei hardFIRE ist eine Instanz notwendig, die mittels der proprietären FPGA-Design-Software spezifische Bitfiles generieren kann. Dies kann beim Administrator selbst erfolgen, wozu dieser allerdings die entsprechende, teure Entwicklungsumgebung des FPGA-Herstellers benötigt.

Alternativ ist eine Aufteilung durch Integration des Firewall-Herstellers denkbar. Hier würden einfache Änderungen, welche kein neues Bitfile erfordern, direkt durch den Administrator am System durchgeführt. Komplexere Modifikationen können standardisiert an den Hersteller kommuniziert werden, welcher daraufhin ein neues Bitfile für den FPGA erzeugt.

Problematisch ist hierbei die Tatsache, dass einer weiteren Partei (dem Firewall-Hersteller) detaillierte Informationen über die Netzwerkinfrastruktur übermittelt werden müssen und der Administrator nur schwer überprüfen kann, ob das Bitfile tatsächlich seinen Anforderungen entspricht. Daher erfordert dieses Vorgehen eine Vertrauensbeziehung zwischen Hersteller und Administrator beziehungsweise dem Endkunden. Mit entsprechender Verschlüsselung und Signierung muss zusätzlich der gesamte Kommunikationsweg von Konfigurationsübermittlung bis zur Übertragung des Bitfiles abgesichert werden.

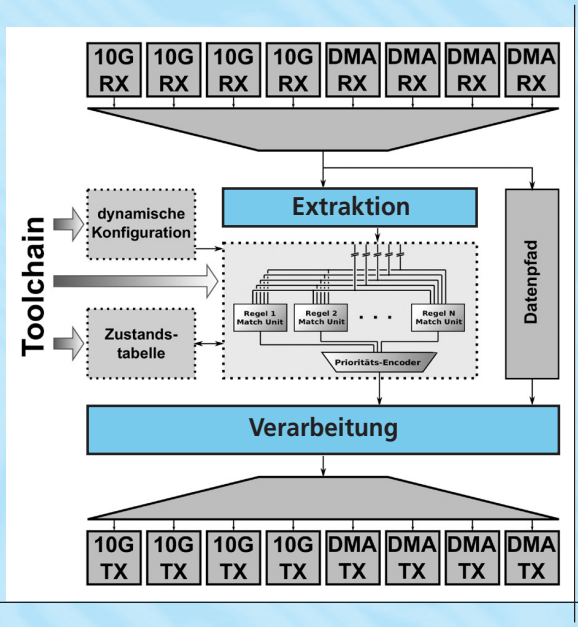


*Abbildung 3: Interner Datenfluss in hardFIRE*

Die im Forschungsprojekt gewonnenen Erkenntnisse und Ergebnisse dienen überdies als Grundlage für eine Vielzahl von verwandten Problemstellungen. Hervorzuheben sind hier besonders die im Projekt behandelten Teilbereiche Stateful Matching sowie die verschiedenen Möglichkeiten zur dynamischen Rekonfiguration. Auf deren Basis können Anwendungen wie Datendioden, komplexe Offloading-Karten, Last- und Hochverfügbarkeitssysteme auf standardisierter FPGA-Hardware realisiert werden.

Die vollständige Version dieses Artikels ist im Kongressband des 14. Deutschen IT-Sicherheitskongresses zu finden [2]. Das Forschungsprojekt wird im Rahmen des Förderprogramms ZIM-KF durch das Bundeswirtschaftsministerium finanziert. ■

## Fazit

Die Performancegewinne einer hardwarebasierten Lösung werden durch den Einsatz eines rekonfigurierbaren FPGAs mit der Flexibilität einer Softwarelösung kombiniert. Da bereits in der Konzeption durch den Workflow eine einfache, transparente Administrierbarkeit vorgesehen ist, kann ein hardFIRE-System mit geringem Aufwand in bestehende Strukturen integriert werden. Mit der Eigenentwicklung der Kernfunktionalität auf Hardware-Ebene und dem Einsatz der beschriebenen Gegenmaßnahmen wird zudem sichergestellt, dass keine versteckten Hintertüren die Firewall kompromittieren können.

## Literatur

[1] Humboldt University of Berlin, genua mbh, Hardfire, Research Project Website, http://hardfire.de/

[2] Andreas Fießler, Alexander von Gernler, Sven Hager, Björn Scheuermann, HardFIRE – ein Firewall-Konzept auf FPGA-Basis, in: Risiken kennen, Herausforderungen annehmen, Lösungen gestalten, Tagungsband zum 14. Deutschen IT-Sicherheitskongress, SecuMedia, 2015, ISBN 978-3-922746-94-2, erhältlich im Buchhandel oder über http://buchshop.secumedia.de/index.php?page=detail&match=LISA_NR2=BSI2015

# Amtliche Mitteilungen

**1. Im Vergleich zur letzten Ausgabe dieser amtlichen Mitteilungen sind inzwischen folgende Zertifizierungen des BSI gemäß Common Criteria und ITSEC abgeschlossen worden:**

| Hersteller/Vertreiber | Produkt | Produkt-Typ | Ergebnis<br>ID<br>Zertifizierungsdatum |
|---|---|---|---|
| MaskTech International GmbH | MTCOS Pro 2.2 EAC with PACE / P60D080PVC - V2 | Smartcard mit MRTD EAC/PACE Anwendung | EAL 4+<br>BSI-DSZ-CC-0892-V2-2015<br>2015-06-30 |
| Infineon Technologies AG | Infineon Security Controller M7892 G12 with optional RSA2048/4096 v1.02.013 or v2.03.008, EC v1.02.013 or v2.03.008, SHA-2 v1.01 and Toolbox v1.02.013 or v2.03.008 libraries and with specific IC dedicated software (firmware) | Smartcard Controller | EAL 6+<br>BSI-DSZ-CC-0891-2015<br>2015-06-30 |
| NXP Semiconductors Germany GmbH | NXP Secure Smart Card Controller P60D080/052/040yVC(Z/A)/yVG including IC Dedicated Software MIFARE Plus MF1PLUSx0 or MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1 | Smartcard Controller | BSI-DSZ-CC-0897-V2-2014-MA-01<br>2015-06-15 |
| NXP Semiconductors Germany GmbH | NXP Secure Smart Card Controller P60x017/041PVD including IC Dedicated Software | Smartcard Controller | BSI-DSZ-CC-0896-2014-MA-01<br>2015-06-15 |
| NXP Semiconductors Germany GmbH | NXP Secure Smart Card Controller P60x080/052/040PVC(Y/Z/A)/PVG with IC Dedicated Software | Smartcard Controller | BSI-DSZ-CC-0837-V2-2014-MA-01<br>2015-06-15 |

**Anmerkung:**
- Die zugehörigen Zertifizierungsreporte mit Zertifikaten sind auf der Web-Seite www.bsi.bund.de/zertifizierungsreporte einzusehen.

**2. Im Vergleich zur letzten Ausgabe dieser amtlichen Mitteilungen ist inzwischen für folgende Produkte eine Zertifizierung beantragt worden:**

| Antragsteller | Produktname | Produkttyp | Zertifizierungs-ID |
|---|---|---|---|
| secunet Security Networks AG | secunet wall packet filter, Version 5.1.0 | Paketfilter | BSI-DSZ-CC-0991 |

**Anmerkungen:**
- Eine Veröffentlichung dieser Angaben erfolgt hier nur, sofern der Antragsteller damit einverstanden ist *und* die Evaluierung begonnen wurde. In der Liste vorhandene Nummerierungslücken betreffen beantragte Zertifizierungen, für die die genannten Voraussetzungen fehlen.
- Bei einigen Produkten handelt es sich um eine Re-Zertifizierung eines bereits zertifizierten Produktes wegen Änderungen am Produkt oder Wechsel der Prüfkriterien.

### 3. Vom BSI zertifizierte und registrierte Schutzprofile

| Entwickler | Profilbezeichnung | ID<br>Zertifizierungsdatum |
|---|---|---|
| Bundesamt für Sicherheit in der Informationstechnik | Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use (MR.ED-PP), Version 1.01 | EAL 4+<br>BSI-CC-PP-0087-2015<br>2015-07-14 |
| Bundesamt für Sicherheit in der Informationstechnik | Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110 (EAC2-PP), Version 1.01 | EAL 4+<br>BSI-CC-PP-0086-2015<br>2015-07-13 |
| Bundesamt für Sicherheit in der Informationstechnik | Common Criteria Schutzprofil (Protection Profile) Schutzprofil 1: Anforderungen an den Netzkonnektor (NK-PP), Version 3.2.1 | EAL 3+<br>BSI-CC-PP-0047-2015<br>2015-04-28 |

### 4. Vom BSI erteilte Standortzertifikate

| Antragsteller | Entwicklungs-/<br>Produktionsstandorte | ID<br>Ausstellungsdatum | gültig bis |
|---|---|---|---|
| Sii Sp. z o.o.<br>(Sii Sp. z o.o.) | Sii Sp. z o.o./Branch in Gdansk<br>(Olivia Point & Olivia Tower, 3rd floor) | BSI-DSZ-CC-S-0039-2015<br>2015-06-17 | 2017-06-16 |

### 5. Vom BSI erteilte ISO-27001-Zertifikate auf der Basis von IT-Grundschutz

| Zertifikatsnummer | Institution | Untersuchungsgegenstand | gültig bis |
|---|---|---|---|
| BSI-IGZ-0209-2015 | IT-Dienstleistungszentrum Berlin | Gegenstand der Zertifizierung ist die gesamte technische und bauliche Infrastruktur des ITDZ Berlin an allen Unternehmensstandorten in Berlin inklusive des High Security Data Centers. Zusätzlich wird mit dem SAP-basierten logistisch-kaufmännischen Gesamtsystem (LKG) beispielhaft eine Anwendung mit hohem Schutzbedarf betrachtet, um die Sicherheit der Infrastruktur im Kontext eines konkreten Anwendungsfalls bewerten zu können. Es werden alle zum Betrieb eines Verfahrens mit hohem Schutzbedarf notwendigen IT-Systeme, die dazugehörigen sicherheitskritischen Geschäftsprozesse, sowie Netz- und Kommunikationsverbindungen zertifiziert. Verfahren, die von Kunden in eigener Verantwortung betrieben werden oder die das ITDZ Berlin in der Verantwortung des Kunden betreibt sowie das Landesnetz Berlin sind nicht Bestandteil des Untersuchungsgegenstandes. | 2018-07-05 |
| BSI-IGZ-0207-2015 | Ministerium für Energiewende, Landwirtschaft, Umwelt und ländliche Räume des Landes Schleswig-Holstein (MELUR) | Der Untersuchungsgegenstand beim MELUR umfasst den IT-gestützten Einsatz der Fachapplikation ZIAF für die Bearbeitung von Förderanträgen im Rahmen der von der Europäischen Union eingerichteten EGFL und ELER-Fonds. Der IT-Verbund beinhaltet eine verzweigte Client-Server Umgebung, für deren Betrieb unterschiedliche Organisationen verantwortlich sind. Dienstleister für den Betrieb der zentralen Komponenten und die Administration eines Großteils der Clients ist Dataport. Der Untersuchungsgegenstand umfasst auch das Änderungsmanagement, das Test- und Freigabeverfahren, die Benutzer- und Rechteverwaltung sowie die Überwachung und Kontrolle des lauffähigen Betriebs der für die Antragsbearbeitung eingesetzten Fachapplikation ZIAF. Der Zugriff vom Client auf die von Dataport betriebenen Server und Applikationen erfolgt von verschiedenen Organisationen unter Einsatz der VPN-Technologie über mehrere Netze. Betrachtet wurden die organisatorischen und technischen IT-Sicherheitsaspekte beim MELUR, den delegierten Stellen sowie bei dem Dienstleister Dataport. | 2018-06-17 |