Informationssicherheit in Deutschland, Österreich und der Schweiz 2015

Eine Studie zur Informationssicherheit in deutschen, österreichischen und Schweizer Unternehmen und Organisationen.

Im Rahmen der Studie wurden in einer **Online-Umfrage** mit **21 fachspezifischen Fragen 229 Teilnehmerinnen** und **Teilnehmer** zu der **Informationssicherheitssituation** in ihrem Unternehmen befragt (56 Deutschland, 82 Österreich, 65 Schweiz, 26 Sonstige).Im Folgenden werden einige der **wichtigsten Ergebnisse** beschrieben.

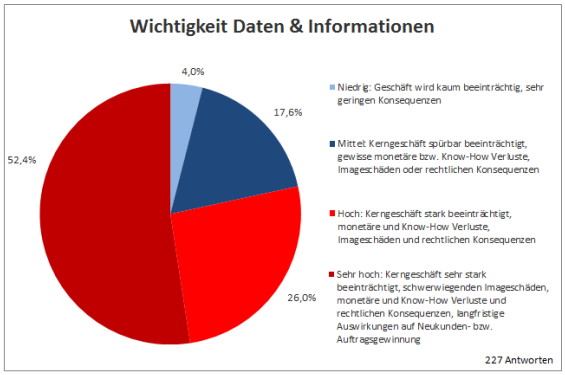
Wichtigkeit der Informationssicherheit

Für mehr als **35%** der Unternehmen ist die **Informationssicherheit „sehr wichtig“** und in allen wesentlichen Geschäftsprozessen ein definierter, integraler Bestandteil, während weitere **40%** die Informationssicherheit als **„wichtiges“ Thema** sehen, für welches eine dedizierte Rolle verantwortlich ist. **Ein Fünftel** empfindet die Informationssicherheit als „**weniger wichtiges“ Thema**, welches hauptsächlich in der IT angesiedelt ist und lediglich für **ein einziges** der teilnehmenden Unternehmen stellt Informationssicherheit ein **„unwichtiges oder nebensächliches“** Thema dar, welches keine besondere Beachtung findet.

Wichtigkeit von Informationen

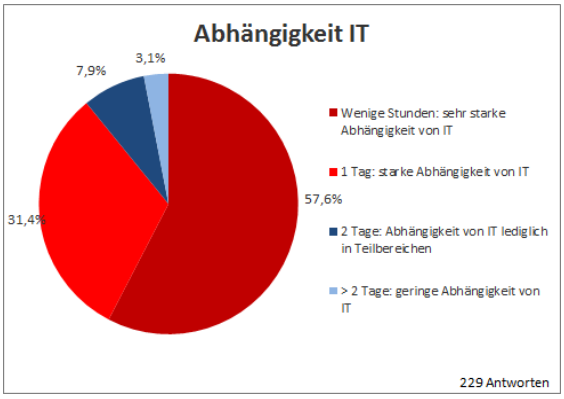
Mehr als die Hälfte der Unternehmen rechnet bei **Verlust, Nichtverfügbarkeit, Verfälschung** oder **unautorisierter Weitergabe** von wichtigen **Unternehmens-Informationen** mit **„sehr hohen“ Auswirkungen auf das Kerngeschäft** (schwerwiegenden Imageschäden, Know-How Verluste, Geldverluste, rechtliche Konsequenzen und langfristige Auswirkungen auf die Neukunden- bzw. Auftragsgewinnung).

Ein **weiteres Viertel** erwartet in solchen Fällen **„hohe“ Auswirkungen** (Imageschäden, monetäre und Know-How Verluste, rechtliche Konsequenzen) für das eigene Geschäft, während nur knapp über **20% der Unternehmen** mit **„lediglich spürbaren“** bzw. **„geringen“ Konsequenzen** rechnet.



Abhängigkeit IT

89% der Unternehmen sind **„sehr stark“** bzw. **„stark“** von der **eigenen IT abhängig**, wodurch bereits bei einem Ausfall von Kernsystemen für wenige Stunden oder einen Tag das Kerngeschäft stark negativ beeinträchtigt oder unmöglich gemacht werden würde. **Lediglich 11%** der Unternehmen sind **„nur in Teilbereichen“** oder in **„geringem Ausmaß“** von der eigenen **IT abhängig**.



Gründe für Informationssicherheit

Die **wichtigsten Gründe** für Unternehmen, sich mit Informationssicherheit zu beschäftigen sind „**Gesetzliche Vorgaben/Compliance**“ (80%), die „**Vermeidung von (Geld/Image)Verlusten durch Sicherheitsvorfälle oder Datenpannen**“ (71%), die **Vorbeugung von „Datenverlusten/Verfälschung“** (69%) sowie die **„starke Abhängigkeit von eigener IT in gewissen Geschäftsprozessen“** (55%).

Probleme bei Aufrechterhaltung und Verbesserung Informationssicherheit

Als Hauptprobleme werden **„fehlendes Budget“** (54%), **„fehlende Unterstützung und Bewusstsein im (Top)Management“** (54%), **„fehlendes Bewusstsein der Mitarbeiter“** (66%), **„fehlende Akzeptanz für Sicherheitsmaßnahmen, welche die Usability/Benutzbarkeit einschränken**“ (65%) sowie „**sich schnell ändernde Systemumgebung und Angriffsarten“** (42%) genannt.

Risiken & Bedrohungen

Hinsichtlich Risiken und Bedrohung, denen sich Unternehmen in Bezug auf Informationssicherheit ausgesetzt fühlen, werden **„Malware** (Viren, Trojaner, Spyware etc.)“ (57%), **„Datendiebstahl“** (49%), **„Fahrlässigkeit eigener Mitarbeiter“** (39%), **„Datenverluste“** (34%) sowie **„APTs“** (30%) und **„Social Engineering“** (30%) am häufigsten genannt.

IS-Policy und Verantwortung

76%

In mehr als **drei Viertel** der Unternehmen gibt es einen **„Informationssicherheits-Verantwortlichen und auch eine Informationssicherheits-Policy“.** In knapp 15% der Unternehmen gibt es zwar eine verantwortliche Person, jedoch ohne unternehmensweite Informationssicherheits-Richtlinie und **lediglich in 10%** der Unternehmen ist **weder die Verantwortung, noch eine Richtlinie definiert.**

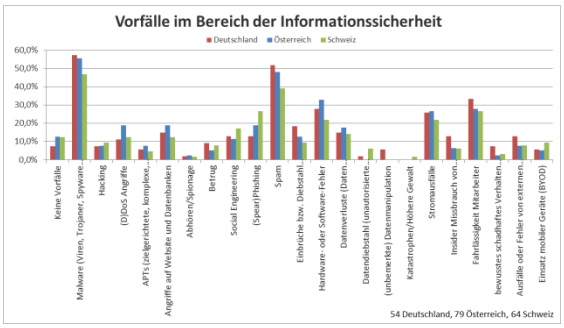
Nutzung von Standards

Am **häufigsten** werden **„ISO 27001“** (69%), **„BSI - IT-Grundschutz“** (52%), **„ITIL“** (49%) und „**COBIT**“ (26%) genannt. Der **„BSI-Grundschutz kompakt“** (31%) sowie die **„OWASP Top 10“** (32%) werden ebenfalls verbreitet genutzt. Auch die relativ neuen „**SANS Critical Security Controls**“ finden bei 11% der Unternehmen Anwendung. **Lediglich 13% der Unternehmen** geben an, **„keine speziellen Standards oder Empfehlungen“** im Bereich der Informationssicherheit zu nutzen.

Informationssicherheits-Vorfälle

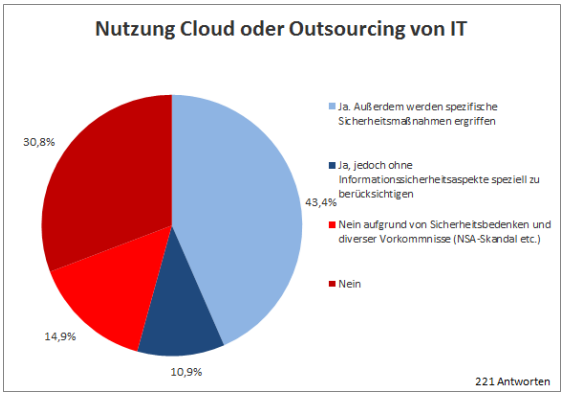
89%

Bei einem **Großteil** von knapp 89% der Unternehmen kam es **im letzten Jahr zumindest zu einem Vorfall** im Bereich der Informationssicherheit. Mit knapp 54% geben **mehr als die Hälfte** der Unternehmen an, dass sie von **„Malware** (Viren, Trojaner, Spyware etc.)“ betroffen waren, während als zweithäufigste Vorfallsart **„Spam“** von 46% genannt wird. Auch die **„Fahrlässigkeit von Mitarbeitern“** (28%), **„Hardware- oder Software-Fehler“** (28%), **„Stromausfälle“** (25%) sowie **„(Spear)Phishing“** (21%) werden häufig aufgeführt. Mit **„Hacking“** (10%), **„Spionage“** (2%), **„(D)DOS Angriffen“** (15%) oder **„bewusst schadhaftem Verhalten eigener Mitarbeiter**“ (4%) wurden anscheinend nur relativ wenige Unternehmen konfrontiert.[1]



Cloud und Outsourcing

Ein **Großteil von 43%** der Unternehmen gibt an **„Cloud und/oder Outsourcing zu nutzen** und dabei **spezifische Sicherheitsmaßnahmen** umgesetzt“ zu haben. Weitere **11%** geben an im Bereich von **„Cloud und Outsourcing aktiv** zu sein, jedoch **ohne Informationssicherheitsaspekte speziell zu berücksichtigen“**. **15%** der Unternehmen erklären Cloud und Outsourcing **„aufgrund von Sicherheitsbedenken und diverser Vorkommnisse (NSA-Skandal etc.)“ nicht zu nutzen**, während weitere **30% keine speziellen Gründe für den Nichteinsatz** von Cloud oder das Outsourcing von IT-Dienstleistungen nennen**.**



Einsatz von Open Source Software

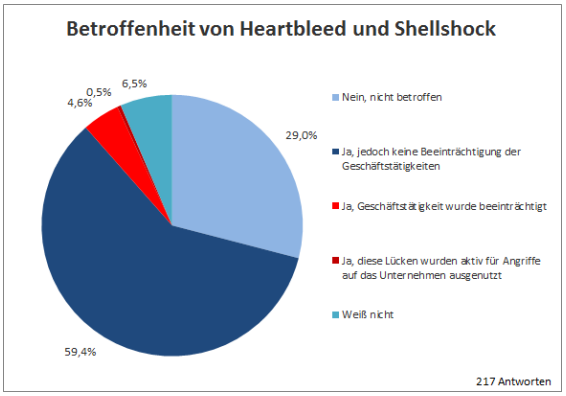
12%

Lediglich **12%** der Unternehmen geben an **„keine Open Source Software“** zu nutzen; nur ein einziges Unternehmen setzt diese aufgrund von Sicherheitsbedenken nicht ein. Die **Mehrheit** von 58% der Unternehmen **setzen Open Source Software ein, jedoch ohne eine (Sicherheits-) Überprüfung** dieser **durchzuführen**. Ein **Viertel** nutzt Open Source Software und trifft dabei **Maßnahmen** wie **„Durchführung von Code Reviews und Recherche zu Auditergebnissen, Sicherheitsanalysen und dem Entwicklerkreis“,** um Sicherheit, Qualität und Vertrauenswürdigkeit zu überprüfen.

Betroffenheit Heartbleed & Shellshock

60%

Hinsichtlich **schwerwiegenden Sicherheitslücken** in Open Source Software wie Heartbleed und Shellshock geben, knapp **60%** an, dass sie **zwar betroffen** gewesen waren, **jedoch** ohne eine **„Beeinträchtigung der Geschäftstätigkeiten" zu erfahren** (etwa durch Nichtverfügbarkeit wichtiger Dienste und außerplanmäßige Wartungsfenster). Nur **5%** der Unternehmen geben an, dass sie von den Lücken **betroffen** waren und hierdurch ihre **„Geschäftstätigkeit beeinträchtigt wurde"**, während für **29% diese Lücken kein Problem darstellten**. Lediglich **ein einziges Unternehmen** gibt an, dass „diese **Lücken aktiv für Angriffe auf das Unternehmen ausgenutzt wurden"**.



NSA-Enthüllungen

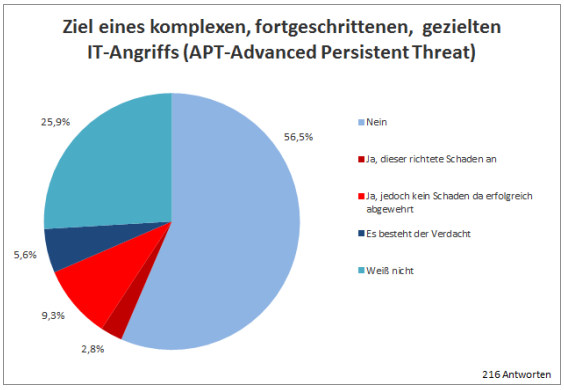
Für **40%** der Unternehmen sind „die NSA-Enthüllungen bezüglich Überwachung und Spionage sowie der gezielten Manipulation von (amerikanischen) Soft- und Hardware-Produkten **kein Thema**", während für **37%** diese Entwicklungen **Relevanz haben** und zu einer **„wachsende Beachtung des Themas der Informationssicherheit"** führten. Weitere **17%** antworten, dass die NSA-Enthüllungen **„zwar ein Thema waren, jedoch darauffolgend keine gezielten Maßnahmen ergriffen wurden".**

Bezüglich Maßnahmen wird **„verstärkter Einsatz von Verschlüsselung"** (16%), „das setzen **auf heimische/europäische Anbieter** im Fall von **Cloud oder Outsourcing"** (16%) sowie die **„Planung zur verstärkten Beschaffung von IT Made in Austria/Germany/Switzerland bzw. Europe"** (9%) genannt. Eine auf diese Enthüllungen folgende „Erhöhung des IT-Sicherheitsbudgets" wird von lediglich 2% der Unternehmen genannt.

APTs

56%

56% der Unternehmen geben an im letzten Jahr **nicht Ziel „eines komplexen, fortgeschrittenen, direkt auf sie gezielten IT-Angriffs (APTs-Advanced Persistent Threats)"** gewesen zu sein. Knapp **ein Viertel** kann nur mit **„weiß nicht"** antworten, während bei **5%** zumindest ein **Verdacht** bezüglich des Auftretens eines APTs bestand. Dies bedeutet, dass bei etwa einem Drittel der **Unternehmen Unsicherheit bzw. Unwissenheit** bezüglich des Auftretens eines APT besteht („weiß nicht" + „Verdacht"), was natürlich auch der Tatsache geschuldet ist, dass APTs schon ihrer Definition nach komplex und schwer zu identifizieren bzw. nachzuweisen sind. Lediglich ca. **12%** erklären, dass sie **im vergangenen Jahr Ziel eines APTs** waren, wobei **nur bei einer Minderheit von 3%** der Unternehmen durch diesen auch **tatsächlich ein Schaden entstand.**



Technische Aufstellung

Grundlegende wichtige Sicherheitstools (wie Firewalls, Virenschutz, Backupsoftware, Mail AV, Spamschutz, VPNs) sind **beinahe durchgängig vorhanden**, wobei sich aber in Bezug auf **weiterreichende oder speziellere Maßnahmen** ein **gespaltenes Bild mit teilweise schnell sinkendem Implementierungsgrad** zeigt. Einige technisch **komplexe und aufwändige Maßnahmen** (wie DLP, SIEM oder auch (Security) Configuration Management Software) sind **nur bei einer Minderheit der Befragten im Einsatz**.[2]

Organisatorische Aufstellung

Einige Maßnahmen (Spam & Antivirus, Backup und Wiederherstellung) sind **beinahe durchgängig vorhanden**, während **kaum andere Maßnahmen** hinsichtlich deren Verbreitung so offensichtlich wie

gewisse technische Maßnahmen hervorstechen. Zwar werden auch „Physische Sicherheit", „Patch & Update Management“, geregelte „Medien-/Datenvernichtung“, „Dokumentation“, „Change Management“ sowie die Durchführung von „Audits, Penetration Tests & Vulnerability Scans“ häufig genannt, doch gibt es auch Angaben, dass diese „in Planung“ oder „nicht vorhanden“ sind. Einige organisatorische Maßnahmen wie **„Versicherung gegen Cyber/IT-Angriffe“,** ein **„firmeneigenes CERT“, „Durchführung-/Teilnahme** an **Cyber Übungen“** oder der **„Betrieb eines IKS inklusive IT-Kontrollen“** sind **nur bei einer Minderheit der Unternehmen umgesetzt**.[3]

Länderabhängige Unterschiede

In einigen Fragen wie zum Beispiel der Nutzung von Standards, in den Unternehmen umgesetzte Richtlinien, Informationssicherheits-Überprüfungs-aktivitäten, dem Einsatz von mobilen Geräten, der Nutzung von Cloud und Outsourcing sowie der technischen und organisatorischen Aufstellung gibt es **durchaus länderspezifische Unterschiede** zwischen den Antworten der Teilnehmerinnen und Teilnehmer aus der Schweiz, Deutschland und Österreich. Hierbei **erscheinen** die **Antworten von Unternehmen aus Deutschland** und der **Schweiz** meist etwas **„sicherheitsbewusster bzw. stärker in verschiedenste Informationssicherheitsaktivitäten involviert“**.

Limitations

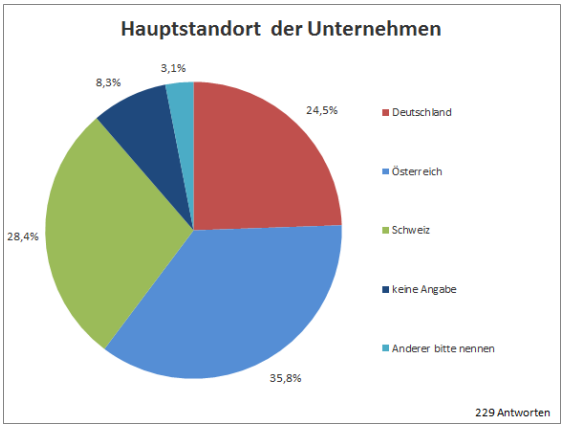
Aufgrund **diverser Einschränkungen** (insb. **Selbst-Selektion**, **Stichprobengröße**, im **Ländervergleich unterschiedliche Stichprobenzusammensetzung**) bei der Verteilung und Durchführung der Umfrage ist eine gewisse **Verzerrung der Ergebnisse** (Über-/Unterrepräsentation von Unternehmen gewisser Größe/Branche bzw. IT-Affinität & Sicherheits-bewusstsein etc.) **möglich und wahrscheinlich**.

Es ist davon auszugehen, dass die **meisten Teilnehmerinnen und Teilnehmer** dieser Umfrage ein **höheres Bewusstsein und Interesse** für das Thema der **Informationssicherheit** aufweisen und hierin **besser aufgestellt sind als ein „typisches, durchschnittliches Unternehmen“**.

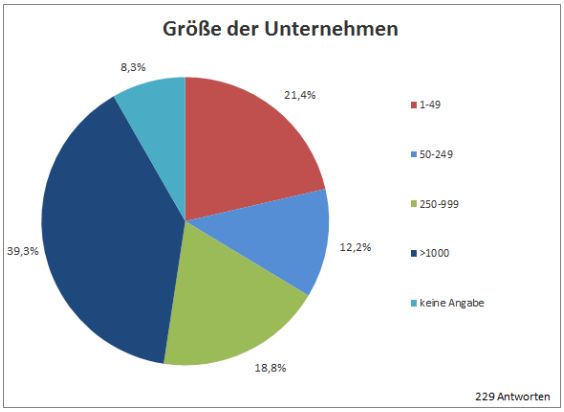
Daher erhebt diese Studie **keinen Anspruch auf Repräsentativität** und die **Gesamtsituation der Informationssicherheit in Deutschland, Österreich und der Schweiz** könnte, verglichen mit den in dieser Studie angeführten Ergebnissen und Schlüssen **„anders“ bzw. „schlechter“ sein, als hier nahegelegt wird.**

Teilnehmerfeld

An der Umfrage nahmen **229 Teilnehmerinnen und Teilnehmer** in Unternehmen aus **Deutschland (56), der Schweiz (65)** und **Österreich** (82) teil (26 Sonstige).



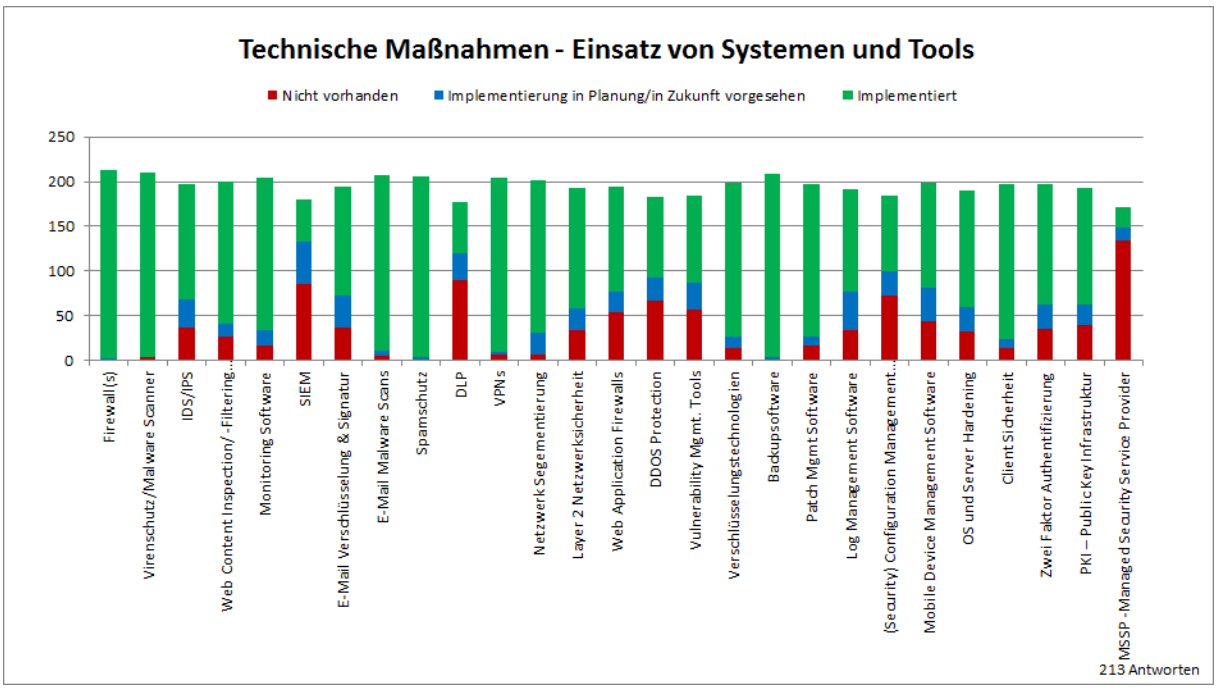
Im Teilnehmerfeld befinden sich Unternehmen unterschiedlicher Größe. **21%** der Unternehmen sind Kleinunternehmen mit **1-49 Angestellten**. **12%** der Unternehmen hatten zwischen **50-249 Angestellten**, während weitere **12%** **250-999** Personen beschäftigen. **39%** der teilnehmenden Unternehmen sind große Unternehmen mit **mehr als 1000 Angestellten.**



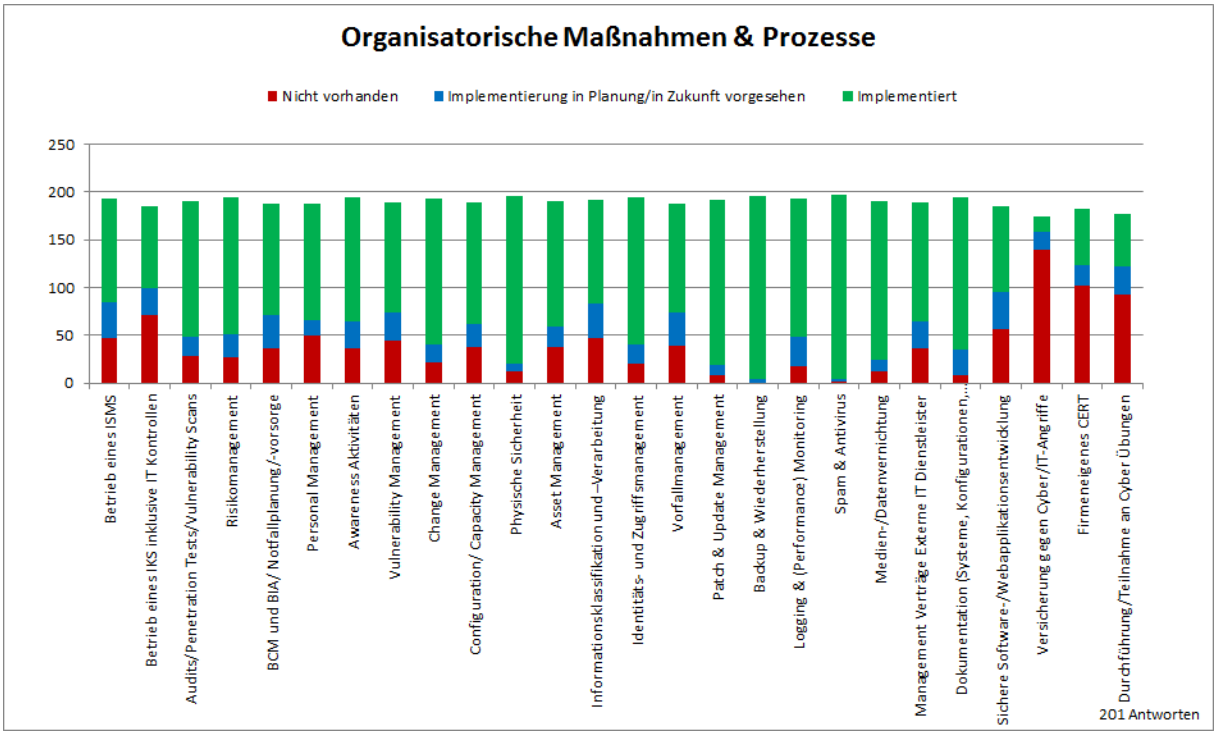
[1] Zur Möglichkeit einer hohen Dunkelziffer und der unterschiedlich guten Erkennbarkeit verschiedener Vorfallsarten siehe Studie Seite 58.

[2,3] Für eine Detailübersicht über in Unternehmen umgesetzte technische und organisatorische Maßnahmen siehe nächste Seite.

Detailübersicht technische Aufstellung



Detailübersicht organisatorische Aufstellung



Kontakt

Bei Fragen oder Anmerkungen stehe ich Ihnen gerne zur Verfügung. Philipp Reisinger, is131510@fhstp.ac.at.