Cyberawareness - Sensibilisierung von Cybercrime auf Geschäftsführungsebene in mittelständischen produzierenden Unternehmen

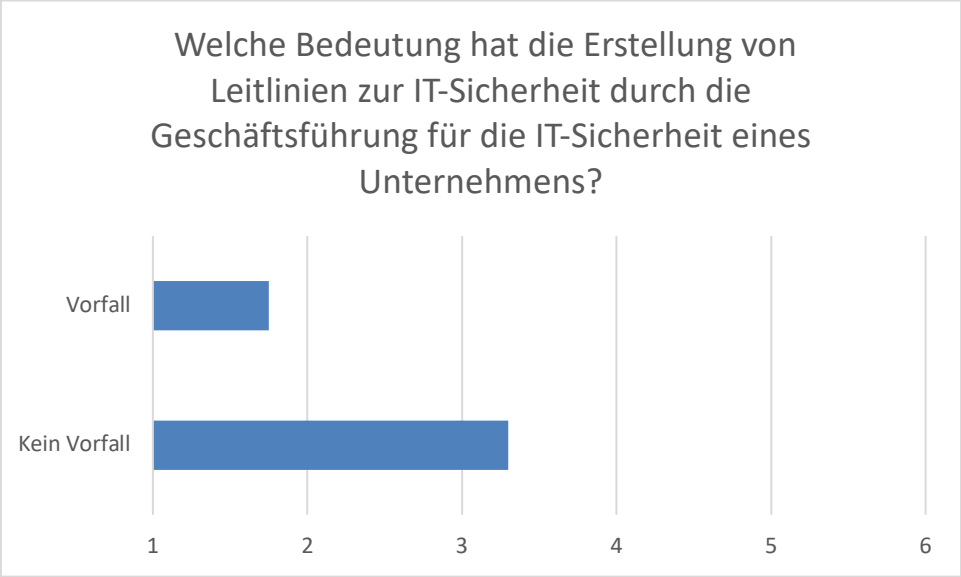
- Anhang -

Thorsten Eller[1], Ramon Rank[2]

Ergebnisse im Einzelnen zu den Fragen

Fragen 1-7 – Organisatorische Maßnahmen

Frage 1:

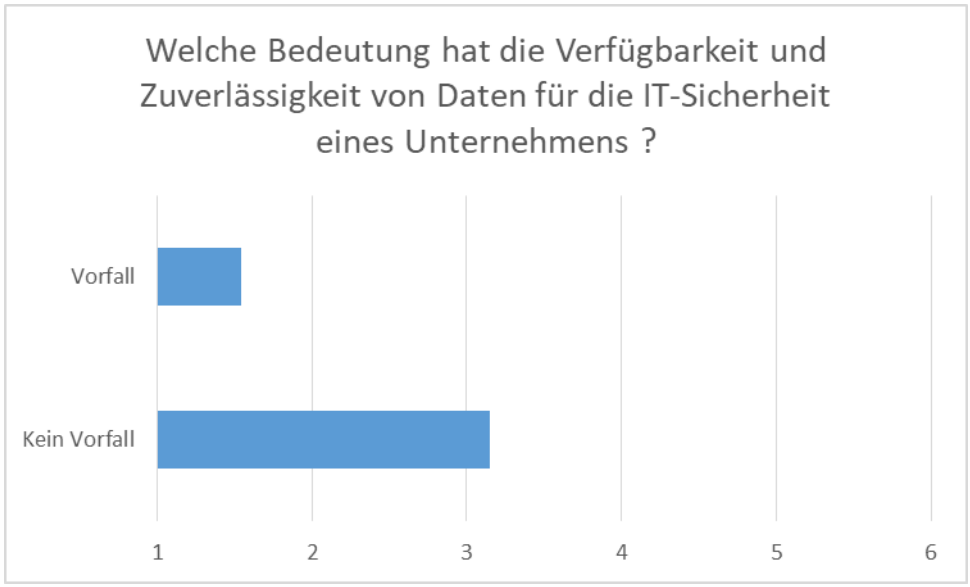


Die Umfrageergebnisse zeigen, dass die Erstellung von Leitlinien zur IT-Sicherheit durch die Geschäftsführung, für die IT-Sicherheit eines Unternehmens als wichtiger angesehen wird, wenn es bereits einen Sicherheitsvorfall gegeben hat (Note 1,5). In Unternehmen, die noch keinen Vorfall hatten, wird die Bedeutung dieser Leitlinien als weniger wichtig eingeschätzt (Note 3,3).

Frage 2:

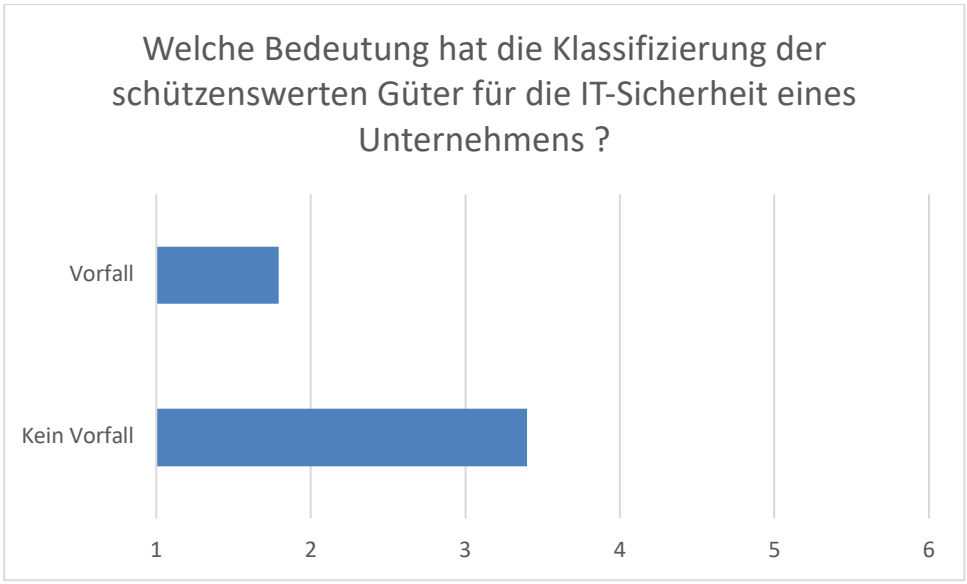
[1] Hochschule Aalen

[2] Industrie- und Handelskammer Ostwürttemberg (IHK)



Die Umfrageergebnisse zeigen, dass die Verfügbarkeit und Zuverlässigkeit von Daten für die IT-Sicherheit eines Unternehmens als wichtig erachtet wird, unabhängig davon, ob es bereits einen Sicherheitsvorfall gegeben hat oder nicht. Allerdings wird die Bedeutung dieser Faktoren stärker betont, wenn das Unternehmen bereits einen Vorfall erlebt hat (Note 1,54) im Vergleich zu Unternehmen ohne Vorfall (Note 3,15). Auf einer Skala von Note 1 bis Note 6 wird die Wichtigkeit der Verfügbarkeit und Zuverlässigkeit von Daten für die IT-Sicherheit als mittelmäßig eingestuft.

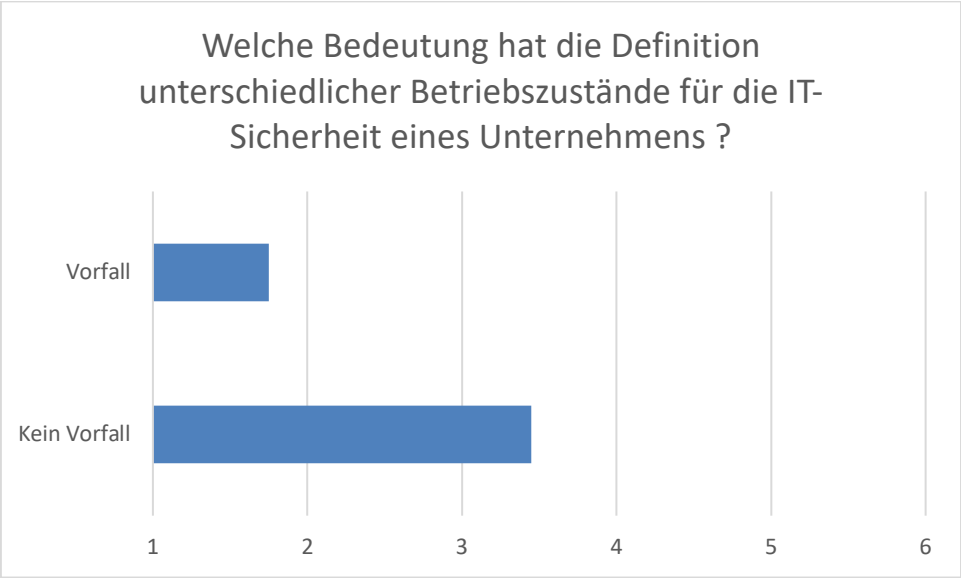
Frage 3:



Die Umfrage zeigt, dass die Klassifizierung der schützenswerten Güter für die IT-Sicherheit eines Unternehmens von den Befragten als wichtig erachtet wird. Unternehmen ohne Vorfall bewerten diese mit einem Durchschnittswert von 3,4, im Vergleich dazu bewerten Unternehmen mit Vorfall die Bedeutung der Klassifizierung mit einem

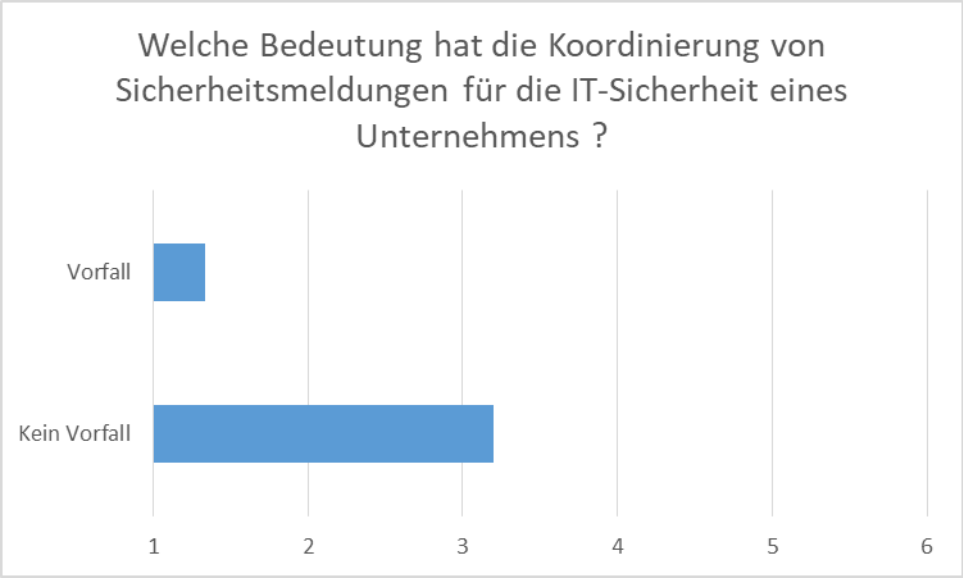
Durchschnittswert von 1,79. Dies deutet darauf hin, dass Unternehmen, die bereits einen Vorfall erlebt haben, die Wichtigkeit der Klassifizierung schützenswerter Güter für die IT-Sicherheit stärker betonen als Unternehmen, die noch keinen Vorfall hatten.

Frage 4:



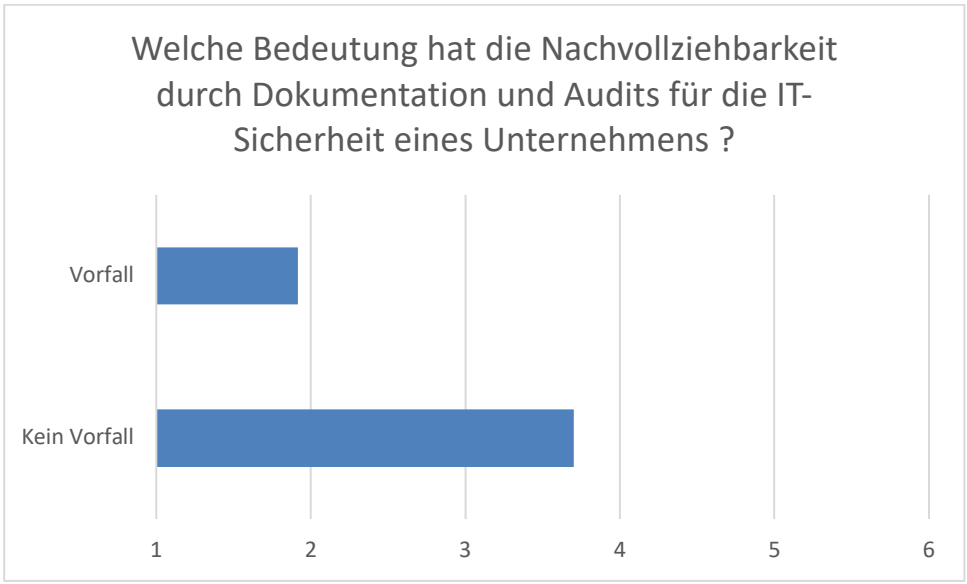
Die Umfrage zur Bedeutung der Definition unterschiedlicher Betriebszustände für die IT-Sicherheit eines Unternehmens ergab bei Unternehmen ohne Vorfall einen Wert von 3,45 und bei Unternehmen mit Vorfall einen Wert von 1,75. Dies bedeutet, dass Unternehmen ohne Vorfall die Definition unterschiedlicher Betriebszustände als weniger wichtig erachten, während Unternehmen mit Vorfall diese als sehr wichtig einstufen. Eine klare Definition von Betriebszuständen kann jedoch dazu beitragen, Bedrohungen schneller zu erkennen und Gegenmaßnahmen effektiver zu ergreifen, was letztendlich zur Verbesserung der IT-Sicherheit beitragen kann.

Frage 5:



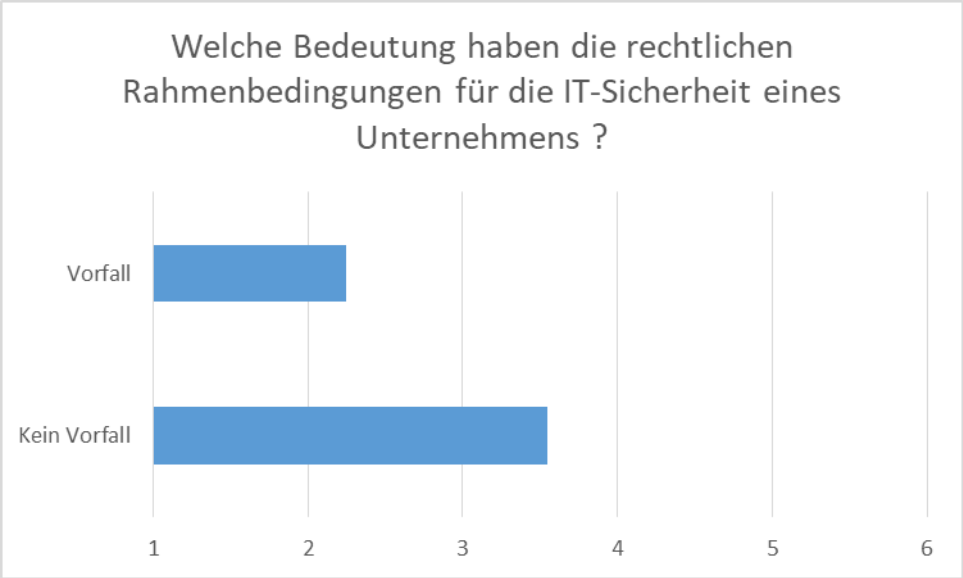
Die Umfrage zum Thema "Bedeutung der Koordinierung von Sicherheitsmeldungen für die IT-Sicherheit eines Unternehmens" ergab bei Unternehmen ohne Vorfall einen Wert von 3,22 und bei Unternehmen mit Vorfall einen Wert von 1,3 auf einer Skala von Note 1 bis Note 6. Das Ergebnis zeigt, dass die Befragten die Koordinierung von Sicherheitsmeldungen für die IT-Sicherheit als wichtig erachten, wobei dieser Aspekt bei Unternehmen mit Vorfall als noch wichtiger bewertet wird als bei Unternehmen ohne Vorfall. Dies deutet darauf hin, dass ein Vorfall dazu beitragen kann, das Bewusstsein für die Bedeutung der Koordinierung von Sicherheitsmeldungen zu schärfen.

Frage 6:



Das Ergebnis der Umfrage zeigt, dass Unternehmen ohne Vorfall die Nachvollziehbarkeit durch Dokumentation und Audits als weniger wichtig für die IT-Sicherheit ihres Unternehmens betrachten als Unternehmen, die einen Vorfall erlebt haben. Dies deutet darauf hin, dass Unternehmen ohne einem Vorfall möglicherweise eine höhere Priorität auf die Etablierung von Maßnahmen zur Verbesserung der IT-Sicherheit legen, anstatt sich auf die Nachvollziehbarkeit durch Dokumentation und Audits zu konzentrieren.

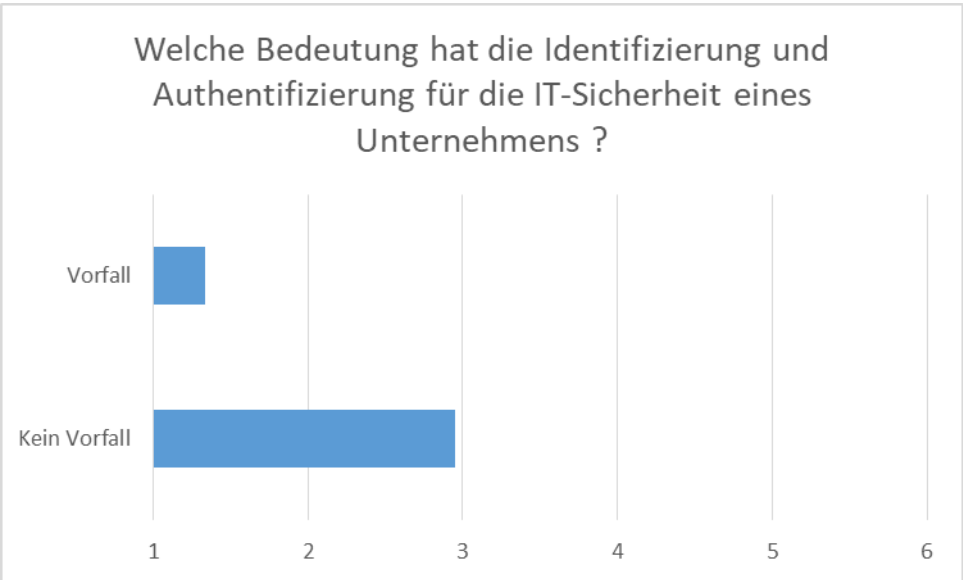
Frage 7:



Die befragten Unternehmen schätzen die Bedeutung der rechtlichen Rahmenbedingungen für die IT-Sicherheit als relativ hoch ein, insbesondere nach einem Vorfall. Unternehmen ohne Vorfall bewerteten die Bedeutung mit einem Wert von 3,55 auf der Skala von 1 ("sehr wichtig") bis 6 ("gar keine Wichtigkeit"), während Unternehmen, die bereits einen Vorfall hatten, einen Wert von 2,25 gaben. Dies deutet darauf hin, dass Unternehmen nach einem Vorfall sich stärker der Relevanz von rechtlichen Rahmenbedingungen bewusst werden und möglicherweise Maßnahmen ergreifen, um rechtliche Vorschriften besser einzuhalten.

Fragen 8 – 13 – Technische Maßnahmen

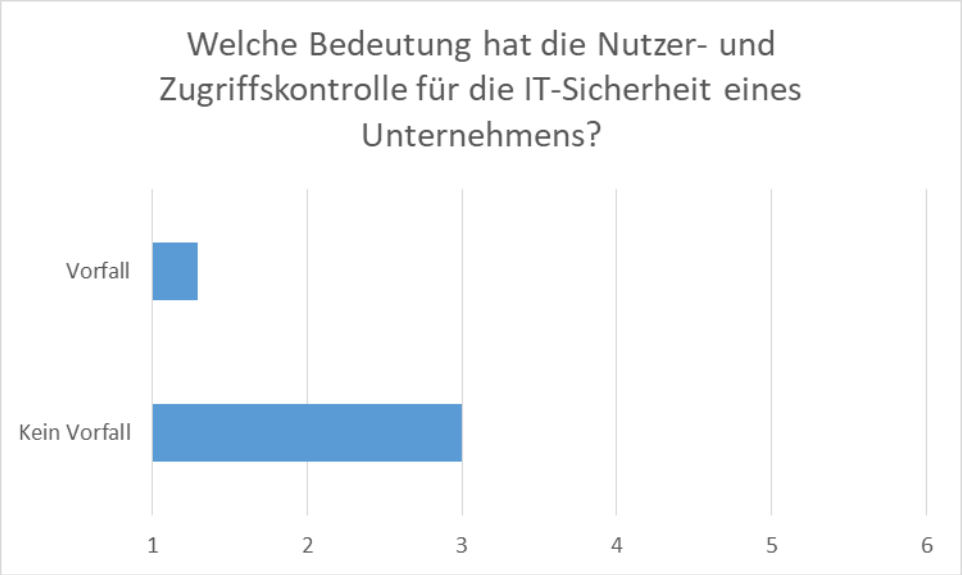
Frage 8:



Die Umfrageergebnisse zeigen, dass die Identifizierung und Authentifizierung für die IT-Sicherheit eines Unternehmens als sehr wichtig erachtet wird. Die Unternehmen ohne Vorfall bewerten dies mit einem Wert von 2,95 auf der Skala von 1 bis 6, während

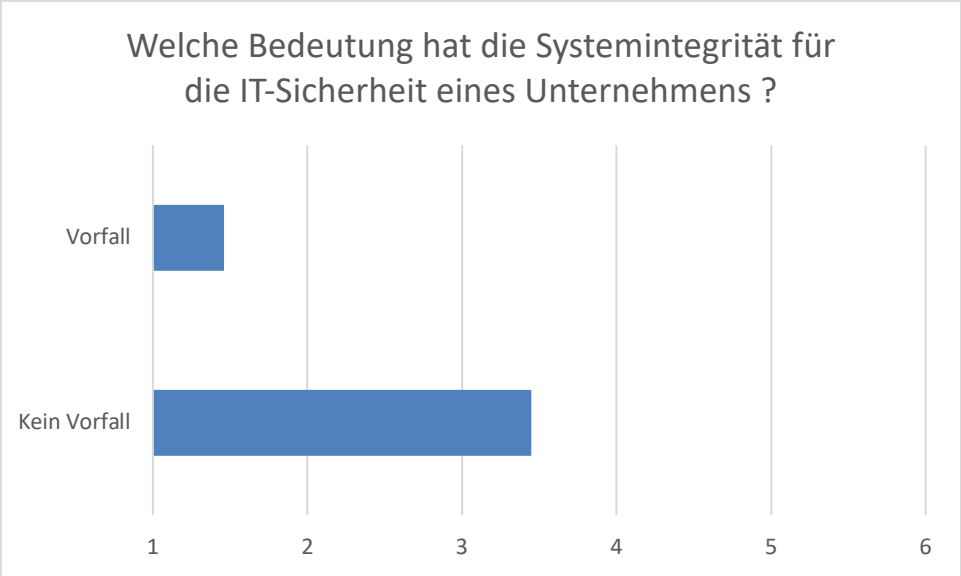
diejenigen mit einem Vorfall dies mit einem Wert von 1,33 bewerten. Dies deutet darauf hin, dass Unternehmen, die einen Vorfall erlebt haben, die Bedeutung von Identifizierung und Authentifizierung für die IT-Sicherheit höher einschätzen als Unternehmen, die noch keinen Vorfall erlebt haben. Eine starke Identifizierung und Authentifizierung kann dazu beitragen, dass nur autorisierte Benutzer auf Systeme zugreifen können, was die Wahrscheinlichkeit von unbefugten Zugriffen und Datenverlusten verringert.

Frage 9:



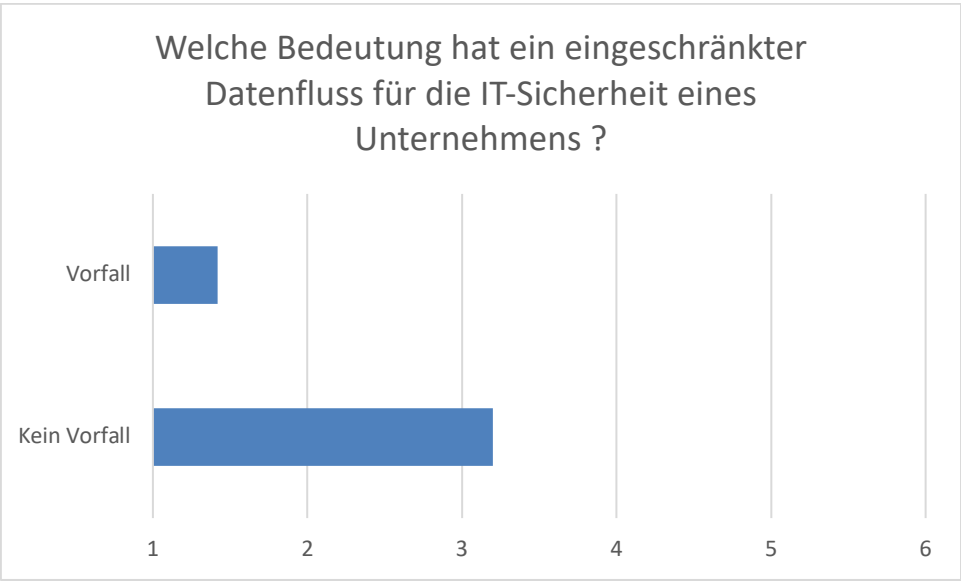
Die Nutzer- und Zugriffskontrolle für die IT-Sicherheit eines Unternehmens wird von den Befragten als sehr wichtig erachtet. Unternehmen ohne Vorfall haben diesbezüglich einen durchschnittlichen Wert von 3 auf einer Skala von 1 (sehr wichtig) bis 6 (unwichtig) vergeben, während Unternehmen, die einen Vorfall hatten, einen deutlich niedrigeren Durchschnittswert von 1,29 vergeben haben. Dies unterstreicht die Bedeutung einer angemessenen Nutzer- und Zugriffskontrolle, um unautorisierten Zugriff auf IT-Systeme und Daten zu verhindern und somit die IT-Sicherheit zu gewährleisten.

Frage 10:



Diw Frage zur Bedeutung der Systemintegrität für die IT-Sicherheit eines Unternehmens, ergab einen Wert von 3,45 bei Unternehmen ohne Vorfall und einen Wert von 1,46 bei Unternehmen mit Vorfall. Das Ergebnis zeigt, dass die Systemintegrität für die IT-Sicherheit eines Unternehmens als wichtig erachtet wird, da der Wert bei Unternehmen ohne Vorfall noch relativ hoch ist. Jedoch zeigt der deutliche Unterschied zum Wert bei Unternehmen mit Vorfall, dass die Bedeutung der Systemintegrität im Falle eines Vorfalls nochmal deutlich höher eingeschätzt wird. Die Ergebnisse legen daher nahe, dass eine hohe Systemintegrität ein wichtiger Faktor für die IT-Sicherheit eines Unternehmens ist, um potenzielle Sicherheitsvorfälle zu vermeiden oder zu begrenzen.

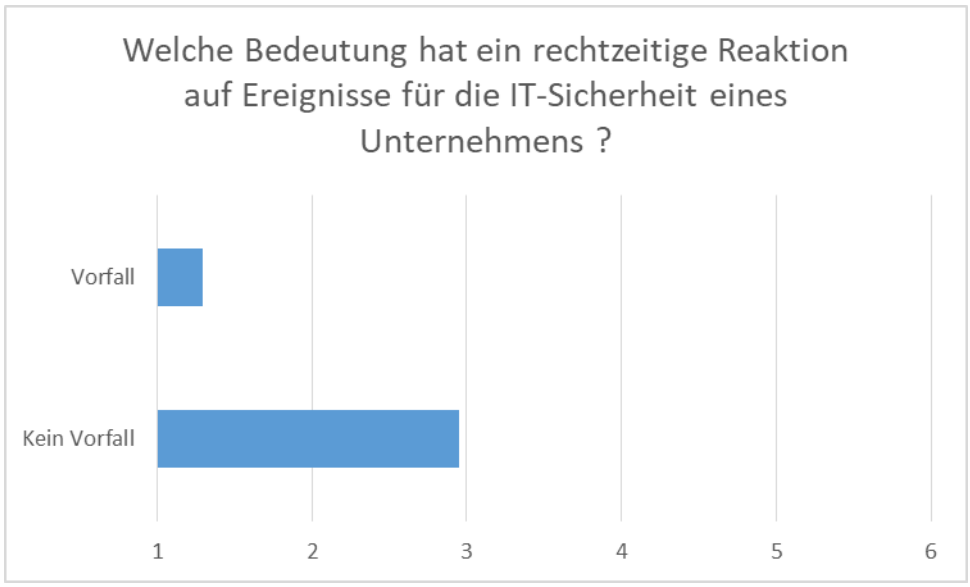
Frage 11:



Die Frage zur "Bedeutung eines eingeschränkten Datenflusses für die IT-Sicherheit eines Unternehmens" ergab, dass Unternehmen ohne Vorfall einen Wert von 3,2 auf einer Skala von 1 bis 6 erreicht haben, während Unternehmen mit Vorfall einen Wert von 1,42 erzielen. Dies bedeutet, dass Unternehmen die Einschränkung des Datenflusses als

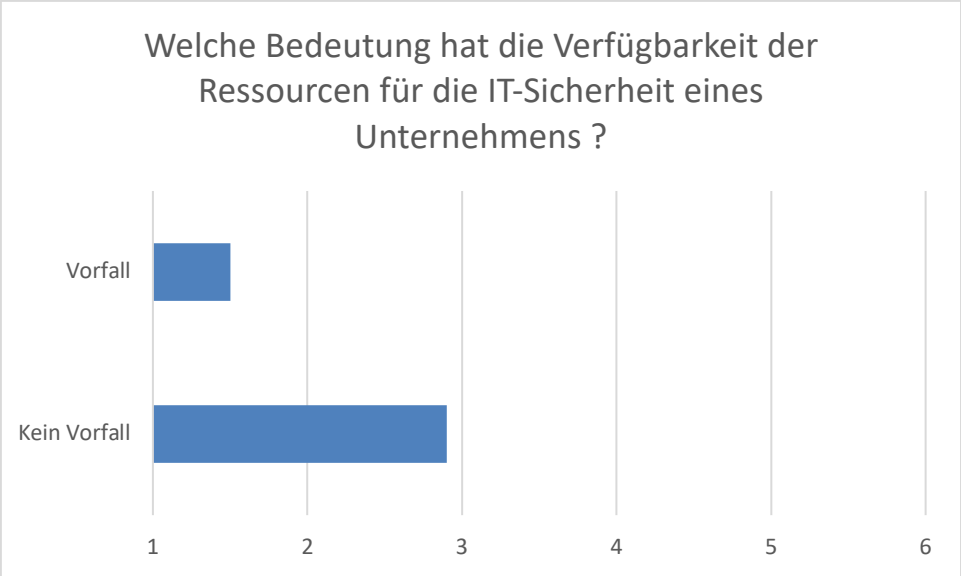
bedeutend für die IT-Sicherheit empfinden, und dass Unternehmen mit einem Vorfall dies als noch wichtiger eischätzen. Ein eingeschränkter Datenfluss kann dazu beitragen, die Wahrscheinlichkeit von Sicherheitsvorfällen zu verringern, indem der Zugriff auf kritische Daten und Systeme beschränkt wird.

Frage 12:



Die Ergebnisse zeigen, dass ein rechtzeitiges Reagieren auf Ereignisse eine hohe Bedeutung für die IT-Sicherheit eines Unternehmens hat. Unternehmen ohne Vorfall bewerteten die Bedeutung mit einer Note von 2,95, was darauf hindeutet, dass sie sich der Bedeutung bewusst sind. Im Vergleich dazu bewerteten Unternehmen, die einen Vorfall erlebt hatten, die Bedeutung mit der Note von 1,29, was darauf hinweist, dass sie erkannt haben, wie wichtig schnelles Handeln im Falle eines Sicherheitsvorfalls ist. Eine schnelle Reaktion kann helfen, den Schaden zu minimieren und die Wiederherstellung des normalen Betriebs zu beschleunigen.

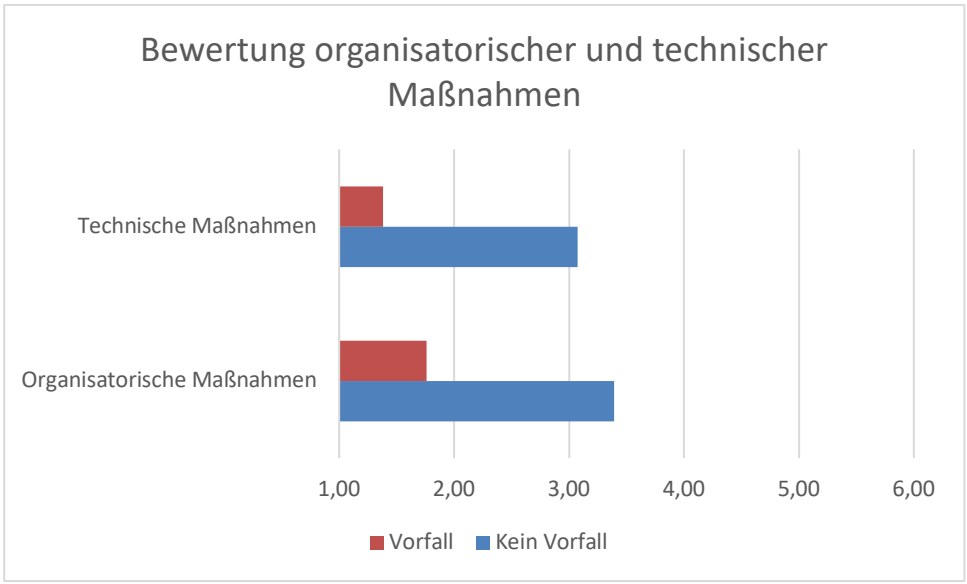
Frage 13:



Die Ergebnisse deuten darauf hin, dass die Verfügbarkeit der Ressourcen für die IT-Sicherheit eines Unternehmens eine hohe Bedeutung hat. Unternehmen ohne Vorfall bewerten dies mit einer Note von 2,9, was zeigt, dass es als wichtig erachtet wird, aber noch Raum für Verbesserungen besteht. Unternehmen, die bereits einen Vorfall erlebt haben, bewerten die Bedeutung der Ressourcenverfügbarkeit für die IT-Sicherheit mit der Note von 1,5. Dies zeigt, dass sie den Wert einer schnellen Wiederherstellung von Systemen und Daten nach einem Vorfall erkannt haben und bereit sind, in diese Ressourcen zu investieren.

Fazit:

Die Befragung zur Bedeutung von IT-Sicherheitsmaßnahmen in Unternehmen hat gezeigt, dass verschiedene Faktoren einen signifikanten Einfluss auf die IT-Sicherheit haben. Die höchste Bedeutung haben dabei die Sensibilisierung und Schulung der Mitarbeiter sowie die regelmäßige Durchführung von Updates und Patches. Die Klassifizierung der schützenswerten Güter sowie die Definition unterschiedlicher Betriebszustände sind ebenfalls von großer Bedeutung für die IT-Sicherheit. Eine eingeschränkte Nutzer- und Zugriffskontrolle sowie ein begrenzter Datenfluss tragen ebenfalls zur Sicherheit bei. Eine rechtzeitige Reaktion auf Ereignisse und die Dokumentation durch Audits und Nachvollziehbarkeit haben ebenfalls einen positiven Einfluss auf die IT-Sicherheit. Rechtliche Rahmenbedingungen sowie die Systemintegrität und die Verfügbarkeit von Ressourcen haben einen mittleren Einfluss auf die IT-Sicherheit. Insgesamt zeigt sich, dass eine ganzheitliche Betrachtung der IT-Sicherheit und ein kontinuierlicher Verbesserungsprozess notwendig sind, um Risiken zu minimieren und IT-Sicherheit in Unternehmen zu gewährleisten.



Das Ergebnis zeigt, dass Unternehmen, die keine Vorfälle hatten, organisatorische Maßnahmen (Note 3,39) als etwas weniger wichtig für ihre IT-Sicherheit erachten als technische Maßnahmen (Note 3,08). Unternehmen, die einen Vorfall hatten, bewerten sowohl organisatorische (Note 1,76) als auch technische Maßnahmen (Note 1,38) als sehr wichtig für die IT-Sicherheit. Der deutliche Unterschied in der Bewertung zwischen Unternehmen mit und ohne Vorfälle zeigt, dass die Implementierung sowohl organisatorischer als auch technischer Maßnahmen von großer Bedeutung für die IT-Sicherheit eines Unternehmens ist.