
***Konzeption eines
IT-Sicherheits-Gütesiegels***
Management Summary

25. April 2017

Management Summary

PwC Strategy& hat im Auftrag des Bundesministeriums des Innern konzeptionelle Eckpunkte für ein Gütesiegel zur Kennzeichnung von IT-Sicherheit erarbeitet. Im Rahmen der Studie wurde eine repräsentative Verbraucherumfrage durchgeführt sowie Interessen und Anforderungen relevanter Hersteller ermittelt und Eckpunkte für die Konzeption erarbeitet.

Das Thema IT-Sicherheit erlangt in der öffentlichen Wahrnehmung eine immer größer werdende Bedeutung. Spätestens seit der Cyber-Angriffe auf hunderttausende Router eines deutschen Telekommunikationskonzerns sowie den „Mirai“-Botnetz-Angriff ist das Thema IT-Sicherheit zunehmend in den Fokus der Bürgerinnen und Bürger gerückt. Um dieser Bedrohungslage zu begegnen, hat die Bundesregierung in der Cybersicherheitsstrategie 2016 unter anderem die Einführung eines Gütesiegels für IT-Sicherheit vorgesehen¹.

Verbraucher fordern Informationen und Orientierungshilfe bei der Kaufentscheidung

In der repräsentativen Umfrage, die im Zeitraum vom 02. bis 08. Februar 2017 stattfand, wurden 1.021 Verbraucher zum Thema IT-Sicherheit befragt.

Die durchgeführte Befragung hat einerseits bestätigt, dass auf Seiten der Verbraucher ein **Informationsbedarf** hinsichtlich IT-Sicherheit besteht, andererseits ein Gütesiegel für IT-Sicherheit das Potential hat, deren Kaufentscheidung zu beeinflussen. Über 90 % der Befragten äußern demzufolge den Wunsch nach mehr Informationen bzgl. der IT-Sicherheit ihrer Geräte.

Ein wichtiger Faktor beim Kauf von internetfähigen Produkten ist für den Verbraucher die „Sicherheit des Gerätes“. So hat die Umfrage ergeben, dass **über 71 % der Befragten, Geräte mit einem Gütesiegel eher kaufen würden** als vergleichbare Produkte und dafür sogar einen höheren Preis in Kauf nehmen würden. Das IT-Sicherheits-Gütesiegel kann daher ein **Abgrenzungsmerkmal** gegenüber „weniger sicheren“ Produkten darstellen und sich infolgedessen am Markt etablieren.

Bezüglich der Frage nach der **Verantwortung für IT-Sicherheit** sehen nahezu 90 % der Befragten die Hersteller und sich selbst in der Pflicht. Hingegen benennen nur 61 % den Staat als die verantwortliche Instanz. Bei der Umsetzung des IT-Sicherheits-Gütesiegels sollte der Hersteller im Fokus stehen, die Verbraucher befähigt werden und der Staat geeignete Rahmenbedingungen schaffen. Letzteres lässt sich ableiten, da die Befragten zu 82 % eine Vergabe des IT-Sicherheits-Gütesiegels durch ein staatlich gefördertes Institut bevorzugen.

IT-Sicherheitsgütesiegel stößt auf hohe Akzeptanz gerade im mittleren Preissegment

Die qualitative Unternehmensbefragung von 18 Herstellern internetfähiger Produkte zeigt ein grundlegendes Interesse an dem IT-Sicherheits-Gütesiegel, als Abgrenzungsmerkmal gegenüber weniger „sicheren“ Produkten.

Vor dem Hintergrund der steigenden Bedrohung internetfähiger Geräte, sehen sich die befragten Unternehmen in der Verantwortung für die IT-Sicherheit ihrer Produkte zu sorgen. Viele binden IT-Sicherheit aktiv in die Produktentwicklung ein und möchten dieses **Engagement dem Verbraucher gegenüber kommunizieren**. Insbesondere Unternehmen im mittleren Preissegment zeigen ein großes Interesse an einem IT-Sicherheits-Gütesiegel als **Möglichkeit zur Produktdifferenzierung**. Qualitätsführer sehen dagegen die Herausforderung, dass ein Gütesiegel die eigenen Qualitätsansprüche nicht erfüllen könnte und somit nicht als ausreichendes Abgrenzungsmerkmal wahrgenommen wird. Unternehmen im Segment der Preisführer stehen dem Gütesiegel zwar positiv gegenüber, die potentiell entstehenden Mehraufwände werden aber als ein zentrales Hindernis wahrgenommen (siehe Abbildung).

¹ Cyber-Sicherheitsstrategie für Deutschland (2016): Bundesministerium des Innern, S. 10

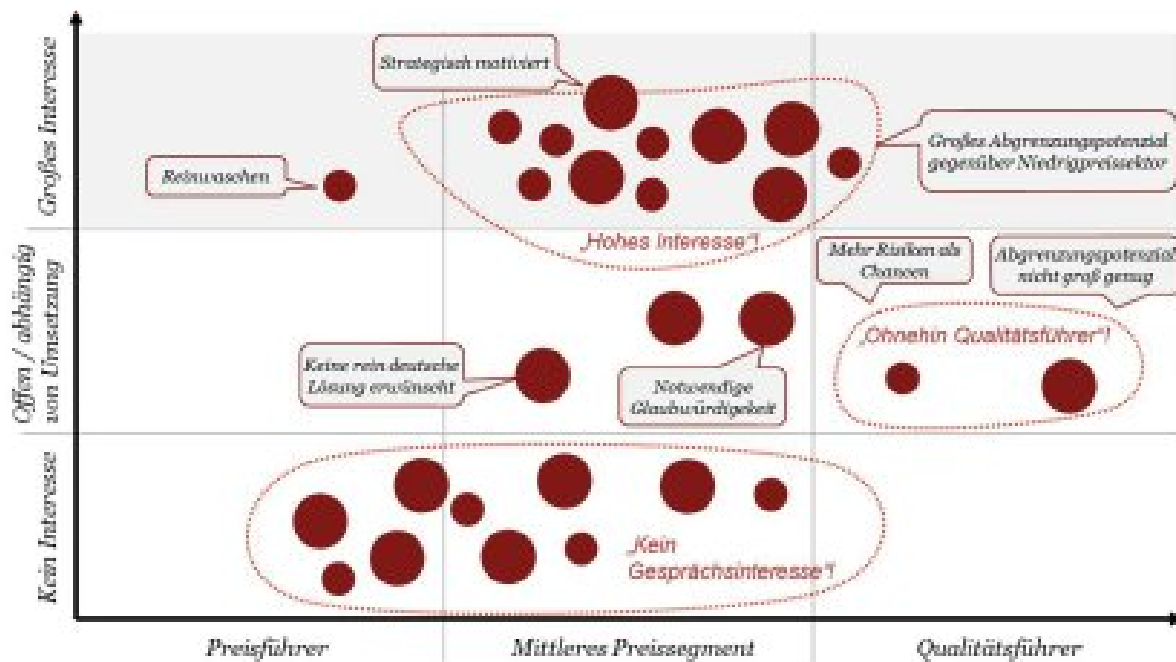


Abbildung: Einordnung der Hersteller hinsichtlich Interesse und Preissegment

Die insgesamt breite **Akzeptanz** für ein IT-Sicherheits-Gütesiegel ist detailliert betrachtet **abhängig von der konkreten Ausgestaltung**. Einerseits muss das Gütesiegel die Komplexität der Thematik abbilden können und das Thema „Sicherheit“ glaubwürdig kommunizieren. Andererseits darf der erzeugte Aufwand nicht den Innovationsprozess der Unternehmen beeinflussen. Entscheidend hierfür sind die Entwicklung einer **anspruchsgerechten Kriteriengrundlage** sowie eine **adäquate Konzeption des Vergabeprozesses** des IT-Sicherheits-Gütesiegels.

Konzeption des IT-Sicherheits-Gütesiegels unter Federführung des BSI

Aus den Ergebnissen der Befragungen lassen sich Eckpunkte für die Konzeption des IT-Sicherheits-Gütesiegels ableiten.

Im ersten Schritt soll das IT-Sicherheits-Gütesiegel dazu beitragen, einheitliche Marktstandards im Bereich IT-Sicherheit zu definieren. Durch eine aufwandsarme Vergabe des Gütesiegels sowie ein transparentes Verfahren, kann eine **hohe Beteiligung** der Unternehmen erreicht werden. Um eine breite Akzeptanz und gleichzeitig Glaubwürdigkeit zu erlangen, sollte das Bundesamt für Sicherheit in der Informationstechnik (BSI), in Zusammenarbeit mit den Herstellern, einen Kriterienkatalog entwickeln. Diesbezüglich können technische, funktionale und prozessuale Kriterien, wie die Etablierung eines Informationssicherheits-Managements und eines Patch-Managements für den Produkt-Lebenszyklus, die Grundlage bilden. Die Ausgestaltung des Kriterienkatalogs wird hinsichtlich verschiedener Produktgruppen variieren.

Hinsichtlich des Vergabeverfahrens hat die Unternehmensbefragung gezeigt, dass die Hersteller unterschiedliche Ansätze bevorzugen, um Verbrauchern zum Kauf von „sicheren“ Produkten zu bewegen. Herstellererklärungen mit Plausibilitätsprüfungen werden aufgrund des geringeren Ressourcenaufwands und der schnelleren Anpassungsfähigkeit an neue Entwicklungen bevorzugt. Im Gegensatz dazu, haben niederschwellige Zertifizierungen mit aufwandsarmen Produktprüfungen den Vorteil, dass sie die Glaubwürdigkeit des Gütesiegels steigern und eine stärkere Produktdifferenzierung nach sich ziehen. Sinnvoll wären hier z. B. Herstellererklärungen inkl. Dokumentenprüfungen sowie selektive Konformitätsprüfungen am Produkt. Mittelfristig sollte ein europaweit einheitliches Verfahren angestrebt werden.

Fazit: Umsetzung des IT-Gütesiegels empfohlen

Die Studie hat gezeigt, dass ein IT-Sicherheits-Gütesiegel den Informationsbedarf der Verbraucher decken und die Kaufentscheidung beeinflussen kann. Folglich kann ein wirtschaftlicher Effekt für Hersteller entstehen, der einen Anreiz zur Teilnahme darstellt. Daraus resultiert das grundsätzliche Interesse der Unternehmen, ihre Produkte durch das IT-Sicherheits-Gütesiegel zu kennzeichnen.

Im Zuge der Einführung eines Gütesiegels für IT-Sicherheit soll ein flächendeckender Standard definiert werden. Des Weiteren soll das IT-Sicherheits-Gütesiegel den Verbrauchern, durch eine transparente und glaubwürdige Kommunikation, Orientierung bieten. Die Hersteller befürworten ebenso die Kennzeichnung von IT-Sicherheits-standards und sehen das Gütesiegel als Abgrenzungskriterium am Markt. Die Akzeptanz durch die Unternehmen ist allerdings von der konkreten Ausgestaltung abhängig.

Im Rahmen der Umsetzung gilt es nun, in einer Kooperation mit Herstellern und Verbänden, den Vergabeprozess und die Vergabekriterien zu entwickeln. Weiterführend sollte zur Einführung des IT-Sicherheits-Gütesiegels eine **Pilotierung für erste Produktgruppen** durchgeführt werden. Aufgrund einer ausgeprägten Verbraucher-relevanz und der hohen Verbreitung bietet es sich an, z. B. Smart-Home-, Smart-TV- Produkte und Internetzugangs-Router als erste relevante Produktgruppen für ein IT-Sicherheits-Gütesiegel zu berücksichtigen.