



# Auswahl von Maßnahmen zur Abwehr von Produktfälschungen

Die fortschreitende Virtualisierung der Geschäftsprozesse im Rahmen von e-Business-Anwendungen führt zu neuen Bedrohungslagen in den Supply Chains. Wurde zuvor auf vertraute Geschäftsbeziehungen gesetzt, sind heute häufig wechselnde und anonyme Geschäftspartner Teil der globalen Netzwerke. Hierin liegen, neben wirtschaftlichen Vorteilen durch die erhöhte Agilität, Gefahren durch unbekanntere Schnittstellen und damit Einfallstore für Plagiate.

Gelingt es nicht, die Supply Chain sicher zu gestalten, indem organisatorische und prozessuale Maßnahmen getroffen werden, hilft in vielen Fällen die Implementierung von technischen Merkmalen zur Identifikation von Plagiaten. Aber diese Maßnahmen sind nur dann als erfolgreich zu bezeichnen, wenn Sie nicht nur die ex post Identifizierung von einem Teil eingeschleuster gefälschter Produkte bewirken, sondern das Fälschen der Produkte unattraktiv machen. Ob dies gelingt, hängt jedoch maßgeblich vom Konsumenten ab; ist er nicht daran interessiert, dass die er erwirbt, originale Produkte sind, dann werden Schutzmaßnahmen keinen hinreichenden Nutzen aufweisen. Darüber hinaus sind Schutzmaßnahmen meist nicht von andauernder Wirkung, sondern werden gegebenenfalls durch die Reaktion der Fälscher außer Kraft gesetzt. Diese Halbwertszeit von Sicherheitslösungen erfordert eine zukunftsorientierte Vorgehensweise im Rahmen der Bedrohungsanalyse.

Zudem handelt es sich bei Investitionen in Sicherheit meist um schwer zu bewertende Investitionen, da es nicht erkenntlich ist, ob die Sicherheitsinvestition wirklich ursächlich Schäden verhindert hat.

Sind die Akteure in den Lieferketten zudem eigenständige Unternehmungen, dann bedeutet das Einbringen von technischen Merkmalen Abstimmungsbedarf bzw. Standardisierte Verfahren dürfen aber nicht zu einer starken Verkürzung ihrer Wirkung führen, sondern sollten durch ein spezifisches Sicherheitskonzept nachhaltig gestaltet werden. Ein analoges Beispiel ist das asymmetrische Verschlüsselungsverfahren in der IT, das z.B. zur Verschlüsselung von E-mails genutzt wird. Hier liegt die Sicherheit in der Länge der Schlüssel, Verfahren und Algorithmen sind öffentlich.

Um nun eine Entscheidung zugunsten des proaktiven Einsatzes von Merkmalen zu treffen, bedarf es einer genauen Analyse der Bedrohungssituation. Hierzu fehlt es aber zurzeit an geeigneten Modellen, wie sie beispielsweise aus der Informationstechnologie bekannt sind. Die Herausforderungen bestehen insb. in einer ganzheit-



lichen Abbildung der Problemstellung mit dem Ziel, Technologien mit Zusatznutzen zu implementieren. Ein wesentlicher und allgemein attraktiver Zusatznutzen besteht in der Nutzung von Identifikationstechnologien zur Verbesserung der Logistikprozesse. Hier verspricht die RFID-Technologie die größten Synergien.

## Vorgehensweise zur Bewertung von Maßnahmen zur Bekämpfung von Produktpiraterie

Die Analyse zur Bewertung von Maßnahmen muss ganzheitlich erfolgen und erfordert zahlreiche Kompetenzen, die nicht unbedingt im eigenen Unternehmen vorliegen. Im Folgenden werden die wesentlichen Analysekategorien genannt:

- **Bedrohungsanalyse**  
Hierunter fällt die Analyse der Marktsituation, der Fälschungsarten sowie des „Geschäftsmodells“ der Fälscher zur Prognose der Gegenmaßnahmen durch die Fälscher
- **Prozessanalyse zur Identifizierung von möglichen Maßnahmen**  
Hierunter fällt die Analyse von Technologien und Maßnahmen bezogen auf die prozessualen Bedingungen z.B. in der Produktion/Verpackung.
- **Prozessanalyse zur Identifizierung von Zusatznutzen**  
Hierunter fällt die Analyse der Unternehmensprozesse insb. Produktion und Logistik und der Analyse der Wertschöpfungskette zur Identifizierung von unternehmensübergreifenden Effekten
- **Erstellung einer Erfüllungsmatrix möglicher Ansätze**  
Hierunter fällt die Analyse der Technologieansätze (versteckte oder offene Merkmale, maschinenlesbare Technologien, wie RFID oder forensische Verfahren, wie etwa Mikroprinting), aber auch organisatorische Maßnahmen.

## Kompetenzzentrum an der TH Wildau (FH)

Die umfangreichen Anforderungen zur bedarfsgerechten Bewertung von Bedrohungen und Maßnahmen unter Berücksichtigung der Einbindung des Unternehmens in das Marktumfeld erfordern eine angepasste Vorgehensweise. Um sichere Identitäten für konkrete Anforderungen nutzbar zu machen und echte Innovation aus den Basistechnologien zu fördern, etabliert sich an der TH Wildau (FH) unter Leitung von Prof. Dr. Frank Gillert ein Kompetenzzentrum für die sichere Objektidentität und -authenticität (COIDA, Competence Center for Object Identification and Authentication).

Das Kompetenzzentrum basiert auf den drei Säulen:

- Produkt- und Markenschutz
- Lifecycle Management
- sichere Supply Chain

Anwendungsfelder sind im Rahmen des Produkt- und Markenschutzes beispielsweise Anforderungsanalysen hinsichtlich des RFID-Einsatzes in den einschlägigen Industrien wie der Pharma-, der Automobil- und der Luftfahrtindustrie.

Fragen im Lifecycle Management betreffen RFID-gestützte Ersatzteilprozesse oder die Freischaltung medizinisch-technischer Geräte.

Im Bereich sichere Supply Chain kann das Kompetenzzentrum auf Forschungsaktivitäten zur Sicherheit im internationalen Containerverkehr mit großen Partnern der Industrie verweisen.

---

Unter dem Dach des Kompetenzzentrums werden die am Hochschulstandort vorhandenen Kompetenzen unter Berücksichtigung des Themas Sichere Objektidentität gebündelt und können mit neuen Synergien verbunden werden. Der Fokus liegt auf dem komplementären Einsatz der verschiedenen Wissenschaften, wie der Telematik, der Biosystemtechnik/Bioinformatik und der Logistik. Die Vernetzung erfolgt mit den Wissenschaftlern des Studiengangs Telematik, die bereits komplementär arbeiten und Know-How bzgl. IKT-Infrastrukturen bieten können. Ebenfalls einbezogen werden die Wissenschaftler des Studiengangs Biosystemtechnik/Bioinformatik. Hier können Testkompetenzen z.B. bezüglich von DNA-Merkmalen in P&M Schutztechnologien genutzt werden, um z.B. Bewertungen durchzuführen.

Neben diesen interdisziplinären Strukturen, die es gilt für das Thema stärker zusammenzuführen, verfügt Wildau durch eine Vielzahl von Forschungsprojekten über Kompetenz im Bereich AutoID/RFID.

Projekte im Bereich der Telematik hatten beispielsweise die Rückverfolgung durch den Einsatz der RFID-Technik in der Transportlogistik bei KMU mit dem Anwendungsfall Kühl- und Frischewaren zum Inhalt.

Darüber hinaus zählen die Entwicklung eines neuen RFID-Standards in der Logistikkette für Druckerei-Druckerzeugnishandel-Bibliotheken, die Grundlagenforschung zur Polymerelektronik für u.a. low-cost RFID-Anwendungen und AutoID Anwendungen in der Forstwirtschaft zu den untersuchten Fragestellungen.

Ausgehend von den Forschungsprojekten ist ein RFID-Labor entstanden, das die Basis für Tests und Entwicklungen von Lösungen mit AutoID/RFID ermöglicht. Seit zwei Jahren veranstaltet die TH Wildau das jährliche Symposium „RFID und Bibliotheken“ und gibt Einblick in Herausforderungen und Chancen von RFID-Anwendungen für Bibliotheken.

Wildau möchte mit der Etablierung des Kompetenzzentrums Lösungen für Bedarfsträger unter Berücksichtigung wirtschaftlicher, gesetzlicher und gesellschaftlicher Fragestellung schaffen. Gleichzeitig geht es um die Rückkopplung mit Politik und Gesellschaft zur verbesserten Gestaltung. Dies soll durch die komplementäre Ausrichtung des Kompetenzzentrums und die Vernetzung mit wichtigen Forschungseinrichtungen erreicht werden. Mit Hilfe einer starken regionalen Vernetzung können darüber hinaus Partner in anderen Regionen angebunden werden. Es ist das Ziel, die Regionen, die ebenfalls starke Kompetenzen besitzen, in Geschäftsmodelle zu integrieren.

Die Tätigkeitsfelder des Kompetenzzentrums reichen von der Forschung, Implementierungsberatung und Industrieberatung bis hin zur Lehre. Ein solches Vorhaben ist von nationaler Bedeutung. Zurzeit ist bundesweit keine vergleichbare Initiative sichtbar, bei aktuell wachsendem Interesse.

**Prof. Dr.-Ing. Frank Gillert**  
Technische Hochschule Wildau [FH]