3D-Druck in der Entwicklung

Revolution des Druckens

Der 3D-Druck wird immer populärer und von der Bevölkerung mit steigender Tendenz als alternatives Herstellungsverfahren zu bewährten Methoden wahrgenommen. In dem 2015 erschienenen Hype-Zyklus[1] wird der 3D-Druck in die drei Teilbereiche Biodruck, Verbraucherdruck und Industriedruck aufgeteilt. Die Anforderungen an die Technik unterscheiden sich je nach Einsatzgebiet erheblich. Der gemeinsame Nenner beläuft sich auf den Empfang komplexer, digitaler Daten und deren Verarbeitung zu realen, physischen Objekten. Formen, die bisher nicht gefertigt werden konnten, werden durch das 3D-Druckverfahren möglich. In den letzten Jahren entstanden technische Gadgets oder Gegenstände wie Prothesen, schussfähige Waffen[2,3] und Schlüsselkopien[4,5]. Geschützte Figuren können als Nachbau auf diversen Plattformen heruntergeladen und gedruckt werden. Zudem steigt mit erhöhter Komplexität eines Systems auch dessen Anfälligkeit für Fehler, wodurch 3D-Drucker ebenso wie Papier-Drucker als Einfallstor in die Unternehmens-IT genutzt werden können. Dadurch eröffnen sich weitere Möglichkeiten für Kriminelle, um Unternehmenswerte zu entnehmen oder zu manipulieren. Die Einhaltung von Integrität, Verfügbarkeit und Vertraulichkeit spielt demnach auch bei 3D-Druckern und der eingesetzten Software eine essenzielle Rolle.

3D-Drucker existieren seit den 80er-Jahren, werden aber erst innerhalb der letzten Jahre verstärkt wahrgenommen. Das hängt damit zusammen, dass Patente ausgelaufen und bewusst nicht aufrechterhalten worden sind. Dadurch wurde der 3D-Drucker für den Markt außerhalb der Industrie geöffnet. Seitdem drängen immer leistungsfähigere und günstigere Geräte für kleine Unternehmen und Endkunden auf den Markt. Geräte, wie 3D-Scanner, sind um den 3D-Drucker herum entstanden und ermöglichen eine subsidiäre Nutzung. Siehe Abbildung 1.

Damit der 3D-Drucker seine Arbeit verrichten kann, benötigt dieser eine 3D-Objekt-Datei, in der ein dreidimensionales Objekt gespeichert ist. Der 3D-Drucker verarbeitet den in der 3D-Objekt-Datei vorhandenen sogenannten GCode, der aus X-, Y-, Z-Koordinationsdaten besteht. Dabei gibt es unterschiedliche Verfahren des Druckens: Neben dem Auftragen von Schichten gibt es auch das Laserstrahl- oder Pulverschichtverfahren. Objekte müssen nicht zwingend aus Kunststoffen wie Polyactiden (PLA) oder Acrylnitril-Butadien-Styrolen (ABS) gedruckt werden. 3D-Drucker sind darüber hinaus in der Lage, verschiedenste Materialien wie Metall, Kupfer oder Beton zu verarbeiten.

Neben 3D-Drucker-Herstellern und Händlern profitieren auch andere Wirtschaftsbereiche von dieser Entwicklung. So entstehen seit einigen Jahren Internetportale, auf denen 3D-Objekte wie Figuren, Tassen und sonstiges Allerlei zum Download angeboten werden, oder Services, die den Druck eines Objekts für Kunden übernehmen. Die Verwendung der 3D-Drucker entwickelt sich aber nicht nur für private Endkunden weiter, auch Unternehmen profitieren von dem Wettbewerb. Ein 3D-Drucker erlaubt Unter-

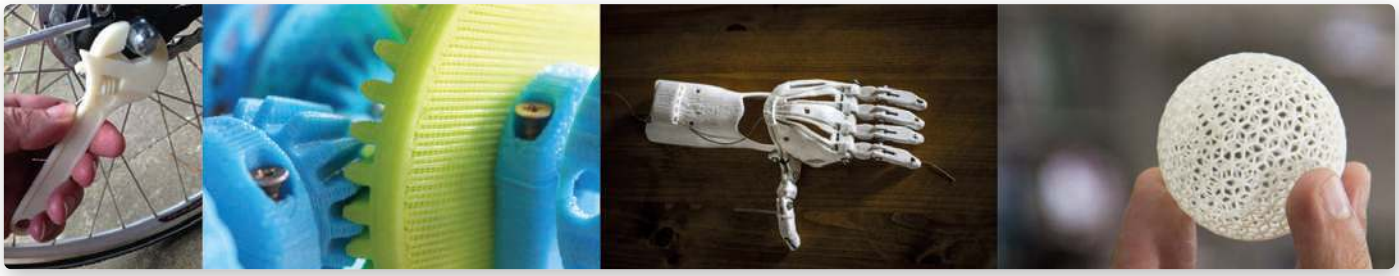

Abb. 1: Beispiele von gedruckten Objekten (Bilder: ifis)

nehmen eine Modifizierung ihrer Herstellungsverfahren, wodurch die Kosten zur Herstellung individualisierter Produkte in der Massenproduktion erheblich gesenkt werden können.

In der Automobilindustrie sollen 3D-Drucker helfen, die Produktionskosten um bis zu 90 Prozent zu senken. Es wurden bereits erste Fahrzeuge komplett per 3D-Druckverfahren hergestellt. Die Flugzeugindustrie hat mit 3D-Metalldruckern begonnen, Bauteile wie Turbinen herzustellen. Im Gegensatz zur hier bewährten Herstellungsmethode, der CNC-Fräse, entstehen mit dem 3D-Druckverfahren kaum Überreste. Besonders ist auch, dass durch die Verwendung von 3D-Metalldruckern und Titan Bauteile bis zu 40 Prozent weniger Gewicht aufweisen. Die NASA hat die Vorteile dieser Technologie ebenfalls erkannt. Positive Entwicklungen sind auch in der Medizin zu beobachten. Zum einen konnten Prothesen für Mensch und Tier kostengünstig gedruckt werden. Zum anderen ermöglicht die Technologie den Druck künstlicher Organe wie Haut und Lebergewebe.[6] Architekten verwenden 3D-Drucker bereits seit Jahren zur besseren Veranschaulichung ihrer Modelle. Wie in den bisherigen Bereichen versuchen Unternehmen Konsumgüter per 3D-Druckverfahren herzustellen. So werden Möbel, Beleuchtung oder Kleidung bereits gedruckt und auf Messen und Modenschauen präsentiert.

Prognosen[7,8] zufolge wurde für 2013 ein Marktvolumen für 3D-Drucker in Höhe von 2,2 Milliarden Euro erwartet, für 2018 werden 4,5 Milliarden Euro und für 2023 7,7 Milliarden Euro erwartet. Bereits Ende 2015 wurden die Erwartungen für 2018 mit 5,1 Milliarden Euro Marktvolumen übertroffen. Dies bestätigt das rasante Wachstum des Marktes und die Wahrnehmung der Chancen, die diese Technologie bietet. Siehe Abbildung 2.

(Un-)Sichere Gegenwart und Perspektive

Die Chancen, die 3D-Drucker mit sich bringen, bergen jedoch auch Gefahren:

- Waffen können gedruckt werden,
- Schlüssel lassen sich kopieren,
- Betrugsmaterialien, wie Karteneinschübe[9] bei Bankautomaten, lassen sich zu Hause produzieren.

Waffen genießen im Zusammenhang mit 3D-Druckern die größte Aufmerksamkeit. Durch die Möglichkeit, privat Waffen zu drucken,[10,11] kann die Registrierung, Steuerung und Regelung von Waffen ausgehebelt werden, und die Schwelle für die Verwendung von Waffen sinkt. Hinzu kommt, dass gedruckte Waffen und Spuren schnell beseitigt sind. Darüber hinaus besteht bei gedruckten Waffen eine Gefahr für den Schützen selbst, da Stabilität und Langlebigkeit bisher eine untergeordnete Rolle spielen. Tests haben gezeigt, dass die bisher druckbaren Waffen qualitative Mängel aufweisen, sodass sie zu Explosionen führen können.

Aktuell existiert keine Lösung, mit der sich Waffen aus dem 3D-Drucker registrieren, steuern oder verbieten lassen. Entsprechende Prozesse, Verfahren und Vorkehrungen müssen eingerichtet werden, bevor der 3D-Druck kritische Nutzergruppen erreicht. Eine manuelle Registrierung gedruckter Waffen ist ein erster Schritt in die richtige Richtung.[12]

Ich druck' mir meine eigene Waffe

Sobald 3D-Drucker und Filamente günstiger und gleichzeitig leistungsfähiger werden, können voll funktionsfähige und sichere Waffen in der Masse hergestellt werden. Gewaltbereite Gruppen sind nicht mehr auf Waffenhändler angewiesen, sondern können ihre eigenen Waffen nach eigenem Bedarf drucken. Der 3D-Drucker ersetzt den Platz aller Beteiligten, die beim Verkauf von Waffen involviert sind. Eine zuverlässige Einschätzung der Stärke von Gruppen und Organisationen lässt sich dadurch, dass kein nachvollziehbarer Waffenhandel stattfindet, nicht zuverlässig vornehmen.

Im Gegensatz zu druckbaren Waffen stellt der Druck herkömmlicher Schlüssel bereits in diesem frühen Stadium der Entwicklung von 3D-Druckern und 3D-Scannern kein Problem dar. Schlüsseldienste, bei denen Schlüssel per Smartphone gescannt werden können, ermöglichen die Speicherung für die digitale Weiterverarbeitung und einen Notfallservice. Bei Verlust des Schlüssels oder Aussperrung aus der eigenen Wohnstätte kann der Schlüssel selbst gedruckt oder binnen kurzer Zeit geliefert werden. Für 3D-Scanner reichen schon einfache Bilder von Schlüsseln aus, um diese ausreichend zu scannen. Studenten des Massachusetts Institute of Technology (MIT) in Boston haben auf diese Weise einen Hochsicherheitsschlüssel eingescannt, gedruckt und erfolgreich angewendet.[13] Ende letzten Jahres wurde auf dem 32. Chaos Communication Congress in Hamburg die Problematik der Einfachheit des Scannens von Schlüsseln anschaulich demonstriert.[14] Für die erfolgreiche Verwendung eines gedruckten Schlüssels waren Metalle als Material nicht zwingend notwendig. Ein günstiges (PLA-) Filament hat für die Herstellung eines funktionsfähigen Schlüssels ausgereicht.

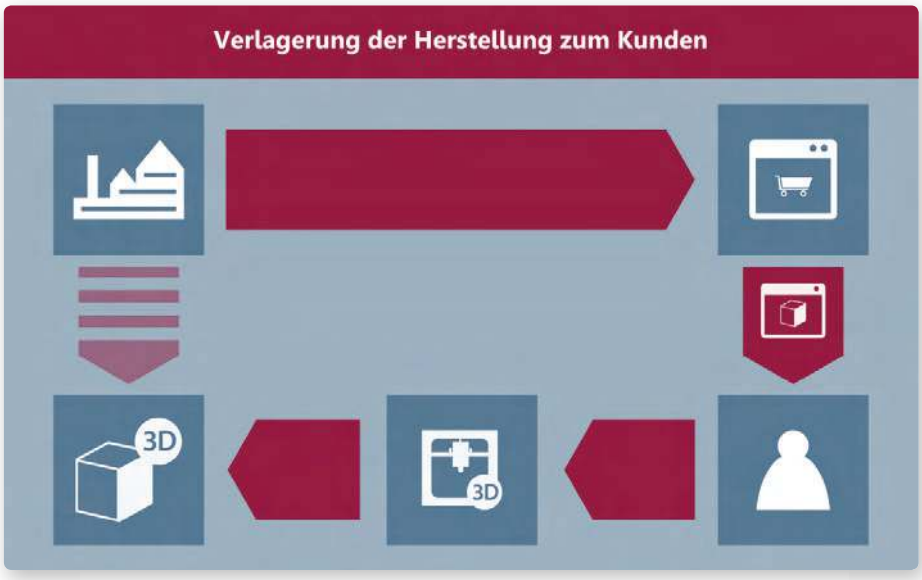

Abb. 2: Prozess des 3D-Drucks (Quelle: ifis)

Probleme mit dem Urheberrecht können entstehen, wenn kostenpflichtige Objekte von Nutzern gedruckt werden, die diese nicht rechtmäßig erworben haben. Dies geschieht beispielsweise durch Vervielfältigung über Filesharing-Plattformen. Vorausgesetzt, dass 3D-Drucker für den Privatgebrauch die Fähigkeit bekommen, Objekte auf ihre legale Herkunft zu überprüfen, wird es auch Malware geben, die sich dieser Fähigkeit entgegenstellt. Eine Möglichkeit wäre das Umgehen der Überprüfung auf dem 3D-Drucker. Eine andere wäre das Manipulieren der Objektdaten, sodass diese vom 3D-Drucker als nicht rechtmäßig erworbene Objekte eingestuft werden. Diese Sabotage kann dazu führen, dass Kunden rechtmäßig erworbene Objekte nicht ausdrucken können. Es kann dadurch der Eindruck entstehen, dass Unternehmen den Kunden 3D-Objekte verkaufen, die einen illegalen Ursprung haben.

Manipulation oder Schwächung der Druckobjekte

Eine weitere Möglichkeit stellt die Sabotage von 3D-Druckern dar. Absichten können sein, Druckaufträge zu verhindern oder – durch eine minimale Manipulation des Druckers – das Ergebnis unbrauchbar werden zu lassen.

Schnell detektierbar sind deutlich fehlerhafte oder ersetzte Objekte. Die Druckobjekte werden durch offensichtlich fehlerhafte oder durch gänzlich verschiedene Objekte ersetzt, wodurch die Produktion aufgehalten wird. Eine Möglichkeit wäre beispielsweise das Auslassen des Henkels einer Tasse. Gegenmaßnahmen können in so einem Fall schnell eingeleitet werden.

Weniger leicht detektierbar sind Schwächungen der Objekte. Die gedruckten Objekte werden an den Rändern oder an anderen kritischen Stellen geschwächt, wodurch ihr ursprünglich geplantes Verhalten nicht mehr gewährleistet werden kann. Bei einer Tasse könnte beispielsweise der Henkel in seiner Stabilität geschwächt werden, wodurch dieser bei Benutzung abbricht.

Keine der neuen Technologien kommt heute ohne Software aus. 3D-Drucker benötigen außer Maus und Tastatur wie klassische Drucker ebenfalls Treiber, um eine Funktion zu erbringen. In der Vergangenheit wurden diese Schnittstellen als Schwachstellen ausgenutzt, um in IT-Systeme einzudringen. Ausgehend davon, dass stabile Software mit einer Fehlerdichte von 0,5 auf 100.000 Zeilen Code noch immer 50 Fehler enthält, entsteht durch die Verwendung eines 3D-Druckers eine potenzielle Angreifbarkeit,[15] entsprechend der Komplexität des Treibers.

Denkbare Angriffsmöglichkeiten wären das Ausspionieren und Manipulieren von Daten. Mithilfe einer Sicherheitslücke, ausgehend vom 3D-Druckertreiber, kann Malware jeglichen Druckauftrag mitschneiden, kopieren und versenden. Andere Marktteilnehmer können auf diese Weise kopierte Produkte schnell und als Original vertreiben. Im schlechtesten anzunehmenden Szenario könnte das Produkt schneller durch den Kopierenden patentiert werden als vom rechtmäßigen Hersteller oder Erfinder.

Sicherheitsmechanismen heute

Bisher werden 3D-Drucker maximal durch Antivirenprogramme, Firewalls oder VPN-Produkte geschützt. Diese Mechanismen dienen in erster Linie dem Schutz des Computers. Drucker profitieren lediglich von Synergieeffekten, die jedoch bei einem gezielten Angriff nicht ausreichen.

Musik- und Filmindustrie als „Vorbild“

Zum Schutz eines 3D-Druckers gibt es bereits einige Lösungen. Ein dänisches Unternehmen arbeitete bereits 2013 an einer Software, die dazu in der Lage sein soll, einen Waffendruckauftrag zu erkennen, diesen zu unterbinden und den Nutzer – analog zur Vorgehensweise eines Antivirenprogramms – mit einer entsprechenden Meldung auf den Umstand hinzuweisen[16]. Waffengegner und Waffenbefürworter vertreten unterschiedliche Meinungen zu dieser Software. Der Entwickler der ersten gedruckten Waffe, Cody Wilson,[17] glaubt nicht, dass eine Software davor schützt, dass weitere Waffen gedruckt werden. Im selben Jahr vertrat der australische Polizeichef auf einer Konferenz ebenfalls die Meinung, dass sich die Verbreitung von Waffendateien und damit der Druck von Waffen nicht verhindern ließen, und stellte einen Vergleich zur Musik- und Filmindustrie auf.[18] Die Verbreitung solcher Dateien zu verhindern, sei nicht möglich. Dafür spricht, dass die originale Datei der ersten druckbaren Waffe innerhalb kurzer Zeit über 100.000 Mal heruntergeladen wurde, bis sie auf Anweisung der amerikanischen Regierung[19] von der Webseite von Cody Wilson heruntergenommen werden musste.

Bezüglich der Software ist es zudem einfach, das Design einer Waffe oder der Einzelteile abzuändern, bis diese von der Software nicht als Waffe oder Waffenteil erkannt wird. Dazu muss beachtet werden, dass ein Einzelteil auch zufällig eine Ähnlichkeit zu den Einzelteilen einer Waffe aufweisen kann. Der Nutzer würde durch die Verhinderung des Drucks eingeschränkt.

Ein japanisches Unternehmen entwickelt derzeit eine Datenbank, in der Muster von Schusswaffen gespeichert werden. Bei jedem Druckvorgang wird die zu druckende Datei mit dieser Datenbank abgeglichen. Bei Übereinstimmung mit der Datenbank wird der Druck verhindert .[20]

Sobald Software dieser Art bedenkenlos und ohne Einschränkung der Nutzer funktioniert, kann nach dem Beispiel des Counterfeit Deterrence System[21], der Fälschungsbekämpfung von Banknoten, ein werksseitiger Einsatz in 3D-Druckern zum Einsatz kommen.

Ideen zu Sicherheitsmechanismen

Eine Möglichkeit, illegale Druckaufträge einzuschränken, kann die Registrierung der Käufer von 3D-Druckern sein. Seit Ende Dezember 2015 werden in den USA alle Käufer von Drohnen mit einer bestimmten Leistung registriert. Darüber hinaus erhalten Drohnen eine Seriennummer zur eindeutigen Identifikation.[22] Ähnlich kann eine Umsetzung auch für 3D-Drucker in Deutschland und anderen Ländern aussehen. Bei der Gesetzgebung sollte in Betracht gezogen werden, dass mithilfe des 3D-Druckers die eindeutig identifizierbaren Teile eines Objekts nachgedruckt werden können. Zur Umsetzung der Registrierungspflicht gibt es unterschiedliche Möglichkeiten: Nach amerikanischem Vorbild kann eine Registrierungswebseite eingerichtet werden, auf der es möglich ist, die Personendaten und die Daten des 3D-Druckers einzugeben. In Deutschland könnte beispielsweise der neue Personalausweis genutzt werden, um den Nutzer eindeutig und beweisbar zu verifizieren. Hilfreich bei der schnellen Umsetzung wäre die Registrierung direkt vor Ort im Geschäft des Händlers. Dies würde dem Käufer zusätzlichen Aufwand ersparen und somit eine Registrierungshürde nehmen. Um Käufer zur Registrierung zu motivieren, wäre ein eingeschränkter Funktionsumfang eine geeignete Maßnahme.

Eine weitere Möglichkeit des indirekten Schutzes bestünde darin, die Nutzung ohne Internetverbindung auszuschließen. Möglich wäre, dass bei jedem Druckauftrag die Internetverbindung dazu dient, den Auftrag mit einer Datenbank abzugleichen und bei Übereinstimmung mit einer Waffe den Druck abzubrechen. Hier stellt sich jedoch zusätzlich zur Frage der Effizienz auch die Frage, wie bei einem solchen Vorgehen mit den Daten umgegangen wird und ob der Betreiber der Datenbank auf diese Weise an Druckdaten gelangen könnte, die nichts mit verbotenen Inhalten zu tun haben. Um zu verhindern, dass die Objekte dem Betreiber beim Abgleich offengelegt werden, könnte mit einem Hashsystem gearbeitet werden. Bei diesem System wird nicht die Datei selbst abgeglichen, sondern der Wert einer Berechnung, der sich aus der Datei ergibt. Dabei findet eine Verrechnung der GCode-Werte statt, woraus sich ein Hashwert ergibt, der Objekte vergleichbar macht. Für die Berechnung wird die komplette Form, sprich die äußere und die innere Form des Objekts, betrachtet. Um auch auf Skalierungen eines Objekts zu reagieren und dieses ebenfalls als verbotenes Objekt zu erkennen, erkennt das Hashsystem einen vorgegebenen Bereich um den Hashwert herum und verwertet diesen Druck ebenfalls. Neben der Skalierung des ganzen Objekts muss auch erkannt werden, ob nur ein Teil des Objekts skaliert wurde. An dieser Stelle müsste das Hashsystem leistungsfähig sein. Designänderungen, wie beispielsweise Änderungen, die nur optischen Zwecken oder dem Umgehen dieses Sicherheitsmechanismus dienen sollen, müssten ebenfalls erkannt werden. Der Mensch erkennt solche Veränderungen relativ einfach. Die Software muss den Menschen an dieser Stelle gleichwertig ersetzen und zu einer künstlichen Intelligenz zur Waffenerkennung werden.

Selektion auch beim Waffendruck notwendig

Bei Einzelteilen einer Waffe muss der Ansatz der gleiche sein, mit dem Unterschied, dass nicht jedes Zahnrad, das für Waffen benötigt wird, in eine „verbotene Liste" aufgenommen wird. Die Vielseitigkeit eines Zahnrads ist groß und muss nicht immer mit der Intention für die Verwendung in einer Waffe gedruckt werden. Vielmehr müssen hier gezielt Einzelteile aufgenommen werden, die existenziell für die Waffenfunktion sind. Falls eine Verhinderung des Drucks dieser Teile nicht möglich ist, kann gespeichert werden, wer den Druckauftrag unternommen hat.

Gegenüber gedruckten Waffen haben herkömmliche Waffen, die innerhalb Deutschlands vertrieben werden, eine Seriennummer,[23] anhand welcher sich der Eigentümer identifizieren lässt. Eine solche Seriennummer könnte automatisch vom Drucker ermittelt und auf erkannten Waffen mit gedruckt werden. Dies wäre eine Option, um beispielsweise sportliche Hintergründe nicht vollkommen auszuschließen.

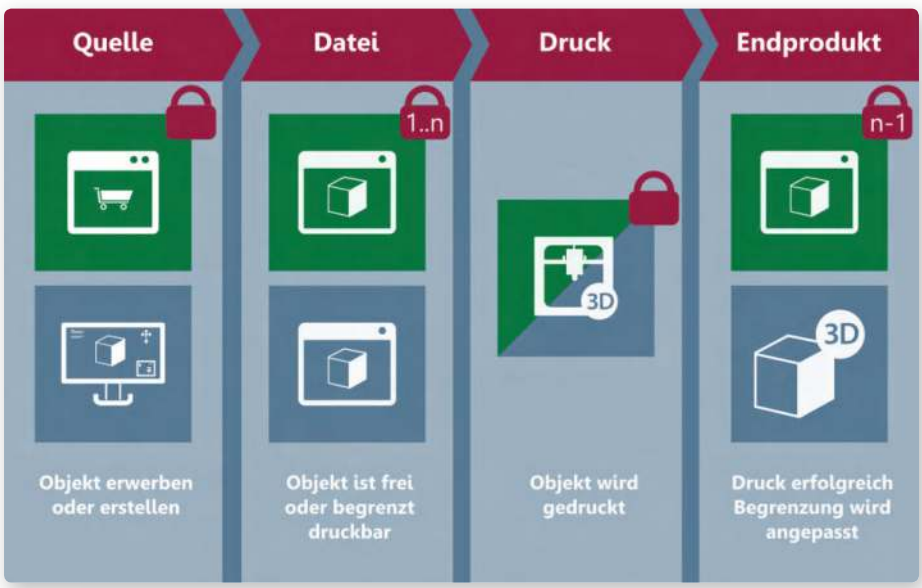

Abb. 3: Schutz von 3D-Objekt-Dateien (Quelle: ifis)

DRM-Verfahren zum Schutz geistigen Eigentums?

Ein weiterer Aspekt ist der Schutz geistigen Eigentums. Objekte sollten nicht frei verfügbar sein oder verbreitet werden können, wenn der Autor dies nicht intendiert. Hier gibt es die Möglichkeit, ein Objekt per Digital-Rights-Management-Verfahren (DRM) zu schützen beziehungsweise zu beschränken. Das Verschlüsselungsverfahren kann angewendet werden, wenn nur ein kleiner Teil Zugang zu den Objekten haben soll. Damit kann auch der 3D-Drucker selbst gemeint sein. Es bestünde die Möglichkeit, 3D-Objekt-Daten verschlüsselt an 3D-Drucker zu senden. Die 3D-Objekt-Daten könnten während des Versands zwar abgefangen, jedoch nicht ohne passenden Schlüssel ausgelesen werden. Eine Verschlüsselungsmethode kann dabei in CAD-Programmen integriert sein. Als digitale Signatur wird die ID des Empfängergeräts mit einberechnet, wodurch eine Entschlüsselung nur am Empfängergerät möglich ist. Erweitern lässt sich die Methode durch Einführung einer Sender-ID in die Signatur. Eine weitere Variante beinhaltet die Einführung von Zertifikaten, wodurch der Zugriff von Unberechtigten auf gesendete 3D-Objekt-Daten weiter erschwert wird. Das System der Verschlüsselung kann auch verwendet werden, um anderen Nutzern oder Mitarbeitern Daten sicher zu senden. Diese Verschlüsselungsmethoden könnten auch von Designservicediensten übernommen werden, um ihre 3D-Objekte sicher an Kunden zu übertragen und eine unentgeltliche Verbreitung zu verhindern. Ein mit Malware infizierter 3D-Drucker, der empfangene 3D-Objekt-Daten sabotieren soll, würde durch Änderungen das Entschlüsseln und Auslesen der 3D-Objekt-Daten verhindern und somit seinen eigentlichen Zweck verfehlen. Dies hätte darüber hinaus zur Folge, dass Material nicht verschwendet würde. Mit der Verschlüsselung ergeben sich jedoch auch Nachteile im Zusammenhang mit dem Waffendruck. Waffendateien lassen sich anhand des Codes nicht ohne weiteres als Waffe erkennen. Siehe Abbildung 3.

DRM-Verfahren können sich beim Verkauf von Objekten in Stores etablieren. Ein solches Verfahren hat sich bei Musik nicht durchgesetzt, was wiederum daran lag, dass

Kunden viele Geräte zum Abspielen ihrer Musik nutzten und die Kopien der Dateien mit dem Verfahren begrenzt waren. Beim 3D-Druck könnte dieses Verfahren optimal eingesetzt werden. Bezogene Objekte werden im Privatbereich im Normalfall nicht massenhaft gedruckt, da dabei Kosten für Filament und Strom anfallen. Eine Verbreitung der 3D-Objekt-Datei an bekannte Personen des Käufers kann mit dem DRM-Verfahren, im rechtlichen Rahmen, beschränkt werden. Für den Fall, dass eine Drucklizenz nachträglich im Volumen erweitert werden soll, kann eine Funktion implementiert werden, die die Aktualisierung ermöglicht. Als zusätzlicher Schutzmechanismus kann das DRM-Verfahren mit Verschlüsselungs- und Zertifikatsmethoden kombiniert werden. Die Infrastruktur des DRM-Systems kann dabei von den jeweiligen Stores selbst betrieben werden oder auch zentral und übergreifend von einer vertrauenswürdigen Organisation.

Die Nutzung von Wasserzeichen stellt eine geeignete Option dar, den Urheber eines druckbaren 3D-Objekts zu erkennen. Die Funktion zur Implementierung der Wasserzeichen in CAD-Programmen integriert, ermöglicht es, anhand von Zertifikaten die Urheberinformationen in Form von Pixeln in einer speziellen Anordnung zu implementieren. Dies ermöglicht den Urhebern die Wahrung der eigenen Interessen. Nutzergruppen können erkennen, von wem das vorhandene Objekt stammt und ob es sich dabei um Originale oder um Imitate handelt.

Fazit

Abschließend lässt sich erahnen, welche Chancen und Risiken mit dieser Technologie einhergehen und wie die Probleme beseitigt werden können – denn Aufgeben stellt keine Option dar. Und sind die Schwierigkeiten erst einmal überwunden, bietet der 3D-Druck die Chance, für die Zukunft salonfähig zu werden und mit ihm Fortschritte und Innovationen zu erzielen. Um das Potenzial vollends auszuschöpfen, ist jedoch eine sichere Technologie Voraussetzung. ■

ARBNOR MEMETI,
wissenschaftliche Hilfskraft am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen im Forschungsbereich „Internet of Things".

PROF. DR. NORBERT POHLMANN,
Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT.

CHRIS WOJZECHOWSKI,
wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen und Leiter des Forschungsbereichs „Internet of Things".

Quellenangaben:

1 *http://www.gartner.com/newsroom/id/3114217*
2 *http://www.forbes.com/sites/andygreenberg/2013/05/05/meet-the-liberator-test-firing-the-worlds-first-fully-3d-printed-gun/#939c735511e6*
3 *http://www.heise.de/make/meldung/Auf-dem-Schiessstand-Die-Pistole-aus-dem-3D-Drucker-1972516.html*
4 *http://www.forbes.com/sites/andygreenberg/2013/08/03/mit-students-release-program-to-3d-print-high-security-keys/#60bb94412da5*
5 *https://media.ccc.de/v/32c3-7435-replication_prohibited#video*
6 *http://phx.corporate-ir.net/phoenix.zhtml?c=254194&p=irol-newsArticle&ID=2209393*
7 *http://wohlersassociates.com/2016report.htm*
8 *https://de.statista.com/statistik/daten/studie/445066/umfrage/prognose-zum-umsatz-mit-additiver-fertigung-weltweit/*
9 *http://krebsonsecurity.com/2011/09/gang-used-3d-printers-for-atm-skimmers/*
10 *http://futurezone.at/digital-life/umstritten-waffen-aus-dem-3d-drucker/24.579.462*
11 *http://www.zeit.de/digital/internet/2013-05/maker-drucker-pistole-internet*
12 *https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB1407*
13 *http://www.forbes.com/sites/andygreenberg/2013/08/03/mit-students-release-program-to-3d-print-high-security-keys/*
14 *https://media.ccc.de/v/32c3-7435-replication_prohibited#video*
15 *Capers Jones: Programming Productivity: 978-0070328112*
16 *http://createitreal.com/download/English%20Press%20Release%20%231.pdf*
17 *http://www.welt.de/vermischtes/article116150584/Cody-Wilson-anarchischer-Schoepfer-des-Befreiers.html*
18 *https://www.youtube.com/watch?v=9taL4svjH_g*
19 *http://www.spiegel.de/netzwelt/netzpolitik/3-d-druck-waffennarren-loeschen-anleitung-fuer-3-d-pistole-a-899024.html*
20 *http://www.dnp.co.jp/eng/news/10118286_2501.html*
21 *http://www.rulesforuse.org/*
22 *http://www.faa.gov/news/press_releases/news_story.cfm?newsId=19856*
23 *https://www.gesetze-im-internet.de/waffg_2002/__24.html*