DSI Industrial & Policy Recommendations (IPR) Series

Recommendations for the Development of Vulnerability Equities Processes

Sandro Gaycken (Digital Society Institute, ESMT Berlin)

Issue 7, 2017

How can the problem be modeled?

Vulnerabilities, also known as "Bugs" or "Vulns", are structural flaws or programming errors that can be exploited by hackers to gain direct access to the systems or to build attacks, so called “Exploits”.

Weaknesses and exploits have been critically relevant to government agencies in the security sector in recent years. In the context of reconnaissance, forensics and surveillance, these agencies must be able to access foreign smartphones and computers. Two variants of this access are strategically and politically undesirable in Germany and are largely technically or legally excluded: the targeted installation of vulnerabilities as "backdoors" in technology products, legally enforced at the manufacturers, and mass surveillance. The installation of backdoors is mainly strategically unwise, as this would severely impair confidence in German technology products on the global market and could lead to a decline in exports. Mass surveillance, on the other hand, is considered in Germany as a serious violation of historically formed ideas regarding the separation of the spheres of the state and of the citizen and, in addition, a violation of the principle of the presumption of innocence.

A third approach, however, is compatible with both of these restrictions. Targeted access to computers or smartphones by hacking the systems (also called “active measures”) neither requires backdoors nor mass surveillance and is structurally much more similar to conventional, pre-digital measures. The author has recommended this as a solution several times in the past in governmental hearings. But this approach is more demanding and more difficult. High levels of competence need to be acquired, vulnerabilities often have limited shelf-lives, and access often needs to be maintained in complicated ways. In addition, the presorting of suspects and the identification of their digital devices without mass monitoring must be achieved by other means. Still: A determined and broad-based cultivation of skills and the use of private sector partners can create a sufficient capacity, which is then more in line with German strategic and political interests.

However, another possible conflict with this approach can be discussed. Normally, whenever vulnerabilities are discovered, they are reported to the software manufacturers so that they can fix them (“patching”). This prevents later or further exploitation of the vulnerabilities by criminals or other malicious attackers. But the vulnerabilities used for state access cannot be reported. They must remain in the products, so they can be used for surveillance, forensics and intelligence purposes. Accordingly, some argue that the use of vulnerabilities by state authorities hurts the larger IT-ecosystem, because those vulnerabilities are not removed and open to all: legitimate state authorities and illegitimate, malicious actors. Accordingly, first ideas and procedures to assess possible consequences of the use of vulnerabilities by the security authorities are emerging. In these processes, known for instance in the USA as the “Vulnerability Equities Process”, competent stakeholders have to assess whether the value of using a vulnerability for security tasks is justifiable compared to the risk of the vulnerability being exploited by criminals and other attackers, or if the risk outweighs the value, so that the vulnerability should be reported rather than exploited. The gain in reporting a vulnerability for patching must be weighed against the gain of its use for active government security purposes.

This paper aims to provide some analysis and commentary on this weighing process by looking more closely at possible procedures, their trade-offs and side-effects.

Should a weighing process be formalized at all?

First insights from documents of the Electronic Frontier Foundation on the American "Vulnerability Equities Process" do not reveal much about how the weighing processes there work. It seems to be a case-by-case decision, by teams of involved or responsible stakehold-

ers. The decision-making process itself is not transparent, but appears to be shaped by regional governmental mentalities. Intelligence services are leading the process, which means that the emphasis seems to be on enabling active government capabilities.

As clear procedures and criteria are not visible yet, the decision-making process will be a political negotiation. It will be subject to typical political dynamics and difficult to predict or retrace in large parts, depending on the number of participants and the length of the proceedings. Influences can arise from political interests above and below them, power and hierarchy structures, the cultures of communication and error, mentalities around security, rotation processes, particularly committed individuals, cooperative interests, the daily press, opposition activities or other similarly volatile factors. Politically trained and more capable entities will have a latent advantage and will be able to better assert their interests.

This non-formal procedure has the advantage of giving the actors a greater scope for action and more flexibility to some extent, as arguments can be introduced outside of a rigid framework. As a result, changes in the relevant strategic field can be better reacted to. However, there is also the risk of wrong decisions, for example, if less competent or unilaterally interested entities with - in one direction or another – misaligned or harmful interests win the negotiation process simply on the basis of their better political competences. In addition, in the current process, accountability and responsibility are hard to pinpoint, leading probably to an inappropriately high risk appetite – a typical problem in the US – or to its contrary, if actors are overly afraid to be made responsible for anything happening somewhere in a rather diffuse and controversial process – a typical German problem. A more formal procedure with concrete, explicit decisions based on lists of specifications and requirements would be needed to achieve more accountability.

A wise solution on how to formalize the process would perhaps aim for a semiformal procedure in which fixed criteria for evaluation must be followed, but without prescribing a decision. The strategic component, which may be important under certain circumstances, would thus have a political right of veto without reducing accountability.

What needs to be evaluated?

As explained above, the gain of reporting a vulnerability for patching must be weighed against the gain of using this vulnerability for governmental hacking in a weighing process. More concretely, the assessment could be determined as "criticality versus value" by considering the *criticality* of a vulnerability for the individual and systemic security of IT against the *value* of this vulnerability for solving crimes or for operational intelligence or military use.

Simple cases would be vulnerabilities where either criticality is very low and value is very high or criticality is very high and value is very low. However, such cases will rarely be unambiguous.

For the assessment of criticality and value, several criteria to be evaluated can be identified.

Criticality:

- Expected CVSS classification and the reasons for it
- Nature and distribution of affected systems (target range)
- Economic criticality of the target range
- Strategic criticality of the target range
- Possible strategic effects
- Possible systemic effects
- Safety criticality of the target range
- Simplicity of exploit development
- Possible technical localities of the effect
- Effectiveness and potential of exploits
- Speed and acceleration of exploit development and deployment
- Usability as stage in modular attacks
- Migration potential of possible exploits with propagation functionalities
- Migration potential of possible exploits without propagation functionalities
- Possible mass effects
- Predictability of effects
- Possible direct damage
- Possible indirect damage
- Possible complex effects
- Possible impairments of safety
- Common case by actor class
- Worst case by actor class
- Cost efficiency for other actors
- Dual-use aspects
- Ease of detection
- Ease of patching
- The manufacturer's willingness and ability to cooperate in patching

Value:

- Relevance of access
- Tactical access requirements
- Depth of access
- Simplicity of access
- Sustainability of access

- Risk of detection
- Distance to relevant vulnerability discovery processes
- Expected shelf-life of the exploit
- Simplicity of exploit development
- Elegance of possible exploits
- Expected exploit quality (e. g. stability, size, process size, functionality, camouflage, platform width, interference with other apps, agility, tunneling)
- Tactical enablement by exploit (e. g. persistence, stealth, modularization, escalation & elevation, interception, exfiltration, trace control, manipulation)
- Forensic value of the exploit
- Number of alternatives
- Comparison of effectiveness, efficiency, cost-efficiency and quality of alternatives
- Exclusivity

Many other criteria would be possible, for example by cross-classification of classical risk assessments such as STRIDE, although a reorientation of these rather technical criteria would have to take place to assess systemic effects in the entire possible target range and to generate comparability.

Another important consideration is the possibility of securing the vulnerabilities (OPSEC), so that they are not stolen or accidentally or intentionally leaked. Especially the leaks of the Shadowbrokers or Vault7 have demonstrated that this can lead to a considerable change in the overall risk and thus also to a significant change in the weighing of criticality versus value. Here, too, some characteristics can be queried whose assessment must contribute to the overall view.

OPSEC:

- Conditions for containment
- Possibility of phased exfiltration of the exploit
- Possibility of operational control
- Possible levels of a cyber OPSEC
- Assurance level of cyber OPSEC
- Possibility of a detection of loss
- Possibility of a detection of misuse by other actors
- Localizability (limitability) of the exploit
- Localizability (limitability) of the attack
- Possible interest of third parties
- Usability for third parties
- Strategic risk in the event of loss
- Risk of detection of current activities
- Risk of attribution
- Risk of post-attribution

Which problems can arise during the weighing process?

Several problems can arise during the process of assessing and comparing criticality and value.

A first problem is the comparison of different categories. For some vulnerabilities, only monetary damage and (in many cases rather hypothetical) losses of privacy can be stated in the view of criticality, whereas in the view of value, human life is often the decisive basis. Vulnerabilities in mobile phones are one example. These allow criminals to steal private data, blackmail people or disrupt services, all of these being rather petty crimes with little damage, whereas prosecutors, intelligence services and the military can closely follow or uncover malicious actors, generating a rather high value for investigations and a prevention of danger to life. Because of this disparity of categories, political preferences will not be completely excluded from the assessment. A different story may arise in more authoritarian countries. They abuse mobile phone vulnerabilities to monitor, control, arrest or murder democratic forces or human rights activists. This, however, does not have to concern us, as these countries are usually heavily biased towards active security in the first place and will rather not report vulnerabilities anyhow.

Another difficulty in weighing is the fact that most criteria need to be evaluated on the most mysterious level of cybersecurity: the level of tactics. Many of the applicable characteristics will have to be considered in their real or possible immediate context, and this can be determined for both, criticality and value, only at the tactical level. Tactical enablement and possible tactical effects must be considered to be able to identify direct and indirect effects, as well as potential strategic damages and consequences. This must also be done in comparison to other variants of tactical procedures. For example, if a particular vulnerability provides a novel tactical option of high value because of an exotic position, while criminals do not require this particular vulnerability as they use different methods in this tactical context, the criticality is less urgent, while the value is higher.

The major problem with tactical level evaluation, however, is the lack of open analysis of this level. In most cases, tactics are only known to those who are operationally active, both offensive and defensive, so a large part of them fall under high secrecy. And even there, “in the know”, the knowledge to systematically evaluate and compare tactics is often underdeveloped and incomplete. In most cases, tactical hackers still tinker their way into a system to apply only a rudimentary set of follow-on tactics of elevation, escalation or

persistence. In addition, tactics often depend on highly variable factors, so an evaluation must always be made and maintained at a very current level.

Does reporting vulnerabilities lead to an increase in IT security?

For many vulnerabilities, which lie between the two extremes "clearly critical" or "clearly high quality", another interesting problem can be indicated, which must be given a little more space in the discussion: the influence of reporting vulnerabilities on IT-security at large. Unfortunately, it is far from certain that the patching of vulnerabilities leads to a maturing of security.

The first doubts may be raised solely based on the number of vulnerabilities. While it has become significantly more difficult for some areas such as the iOS, the Android kernel or some TrustZone implementations to find structurally known vulnerabilities, in other areas such as operating systems, most applications or ERPs, there are still many hundreds to thousands to hundreds of thousands of vulnerabilities to be found. These figures also tend to increase over time in the direction of security maturity, due to new developments with new bugs severely outpacing the removal of old bugs. This is especially relevant in the current digitization mania, with many start-ups with high pressure, little time and no quality assurance producing lots of buggy code on top of the overall IT ecosphere. In addition, according to current statistics, approximately one third of these start-ups have increased CVSS criticality in office IT, and about half in industrial IT.

Consequently, if a normal IT product contains not just a few dozen, but constantly thousands of critical vulnerabilities, and if the development and design patterns continually increase this number, it can be argued that the reporting of individual vulnerabilities will not lead to a significant or sustainable overall increase in security anyhow - even if they have a high level of criticality. Capable and motivated attackers will find a critical vulnerability if they search specifically and systematically, no matter what. And most state authorities require only a very few vulnerabilities per system anyway. This will have a lasting effect on the balance between criticality and value. For most systems, even the reporting of highly critical vulnerabilities will produce no significant increase in overall security, while the value of the vulnerabilities immediately collapses completely.

Unfortunately, the facts for a precise assessment of the systemic security effect are extremely weak. There are no accurate measurements or even well informed estimates available, so only guesstimates based on the few known defect rates and experience of the hacking community can be made.

The gray market prices of exploits could be seen as an indicator for the security maturity of a system and the relevance of reporting vulnerabilities, but these prices are also influenced by a number of other typical market factors, such as existing tools, available know-how, required resources, necessary specialist knowledge, and type of need, so that only qualitative relations may be read off there.

How would a new vulnerability regime affect actors?

Another important question is if more vulnerabilities were actually reported if a weighing process were to be regulated explicitly. This can be judged by considering how actors are likely to change their behavior in the event of explicit regulation.

The intelligence, criminal and military actors who seek vulnerabilities for offensive purposes are under great financial and performance pressure in all countries without exception. In addition, in the area of "hacking", almost all of them have hardly been able to build up any significant competencies, so that only a few good hackers are available at all. In many, even large industrialized countries, these are often no more than a handful to a few dozen people, with little options to scale. As a result, these agencies will not put these very limited and much-needed resources into identifying vulnerabilities that they are not guaranteed to benefit from. They will set up a process of prior evaluation that will examine before the discovery process which vulnerabilities could actually be used actively, and which ones must be reported, so that only those that can be used are worked on. It is therefore unlikely that any vulnerabilities will be reported from these institutions at all. In comparison to the current situation, a net loss would be more likely to result from reporting vulnerabilities. Critical vulnerabilities are currently reported in some cases, as the detection process is not structured to a reporting requirement.

Government agencies could play another role. A more proactive regulatory option would be to set up a government institution of its own to detect vulnerabilities and communicate them to the software industry. However, this government agency would have to reckon with high competition for the available talents, while at the same time facing a much more boring task, and thus hardly have a chance to build up a significant competent workforce. Under normal salary and working conditions, there will be scarcely more than ten to twenty people who are able to find vulnerabilities in large and already post-hardened legacy systems in manual code analysis above the quality of technical analysis tools. This could only be achieved in smaller specialist areas where special expertise can be acquired and where standard analysis tools do not work as well. An example are some fields of industrial IT. In

addition, such a government-funded agency would be exposed to the justified accusation of assuming an expensive and cumbersome task for the IT industry, which in this way can unjustifiably turn its own costs incurred as a result of negligence in quality assurance into costs for the public.

Another actor who would change his behavior would be the gray market of exploit resellers and freelance government hackers. These would only sell with great caution to governments that have a reporting process, unless it can be explicitly and reliably assured that the purchased vulnerability or exploit will not be made public, or they would only sell at exclusive prices which would be on average two to three times the normal prices. Even then, however, some providers could be rather cautious, as a publication of the vulnerability often also provides the manufacturer with conclusions about the methods or perspectives of the hacker, so that the hacker's potential for action and thus the market value are also more fundamentally weakened.

One variation of this actor are hackers who collect bug bounties by reporting vulnerabilities directly to the software industry and not selling them in the gray market, because the value would be below the bounty, or because the grey market is a political no-go, scary or inaccessible to them. These hackers are currently only of secondary importance, since the gray market attracts many more than bug bounty programs, and they would only change their behavior and pass vulnerabilities on to states with reporting processes if they were offered a bounty with higher value or if they were disappointed by the behavior of the software industry. This may currently only apply to a small number of rather less relevant vulnerabilities.

Nor will other companies that routinely report weaknesses to the manufacturers in the software they are running change their behavior. They follow established processes that are unlikely to be affected by a state reporting process.

For software vendors, some implications could arise, but these are still difficult to estimate at present, as the modalities of the cooperation would have to be clarified first. However, if many countries report vulnerabilities, many windows of opportunity will be created and a net loss of security is to be expected, because the manufacturers' ability to patch is already at the end of its capacity.

Should exploits be bought to publish them?

The idea that government agencies buy expensive vulnerabilities from the gray market to report them sounds absurd at first. States acting in this way would parallelize bug bounty programs of the software industry and in the medium term would infiltrate and kill them due to the significantly higher prices with the same outcome. But such thoughts were actually put forward. The federal government of Germany has already been offered vulnerabilities at the BSI, where consideration has been given on how to deal with them. From a legal point of view, the interesting question arises as to whether a legally formalized process of reporting creates an obligation to purchase such vulnerabilities, which in turn could lead to a presumably unfavorable development. A gray market of its own could arise, specifically for the weaknesses regarded by states as critical, with a rather high-priced structure and to the "disadvantage" of the bug bounty programs of the software industry, which could convert their own costs into public costs again.

What are possible global strategic consequences?

The international strategic implications of the resulting asymmetry between countries without a reporting regulation and countries with such a regulation may also become problematic. States without a formal disclosure process will be much less constrained to find vulnerabilities and to develop exploits. They will be faster because they do not have to go through reviews, because they can also use easily found vulnerabilities and because they can use a wider range of talents. They may also be more popular customers for some parts of the exploit gray market.

As a result of these development and procurement advantages, their military and intelligence cyber operations will be much more tactically flexible and agile as they offer them more options and as a different and broader tactical combinatoric approach can be used. Since only a few target ranges would be categorically excluded, the selection of possible strategic options will also be significantly broader and relevant actors could work in many fields that are not accessible to others. In addition, over time, not only the arsenals but also the capabilities of the operators in these countries will become significantly better than those of states with a strong regulation of vulnerability reporting.

Also, it can be assumed that states without a strong civil society, democracy and the rule of law or states in harsher conflict situations are more likely to renounce a reporting process and will also make targeted use of the asymmetric advantages of a stricter vulnerability regime in other countries. Therefore, an asymmetric offensive enablement of authoritarian states could be a direct strategic consequence.

How can the process of state exploit development be made more secure?

There are a number of options to make the state's development of hacker attacks more secure and to improve the relationship between criticality and value. On the one hand, both characteristics should be considered when purchasing and developing or customizing

exploits. On the other hand, all possible procedures for a very high OPSEC must be identified and rigorously implemented.

Finally, there are a number of other options that minimize risks for the wider public.

First, offensive government agencies should prefer to develop and buy high-value and exotic exploits and vulnerabilities. These are less likely to be detected by criminals or other less talented opponents, so that the risk of non-reporting is reduced proportionally. A comprehensive methodology could be developed in this direction, since, fortunately, high-value and exotic exploits can still be identified as categories and since corresponding skills in developers and sellers can be identified as well, as a high degree of competence in this field is required.

Second, offensive government agencies could also seek to identify whether the vulnerabilities they use have been discovered and are being exploited by opponents. Vulnerability-specific indicators of compromise could be developed and deployed in special, diode-protected honeypots to analyze attacks for according indicators. If attacks are identified that could involve a vulnerability in use, the IT industry could be informed accordingly.

Third, offensive government agencies can produce extensive documentation for their own vulnerabilities and develop patches as far as possible externally. As soon as the vulnerability becomes known, this knowledge can be immediately communicated to the IT industry, and it can be assisted in patching to significantly shorten the window of opportunity between a vulnerability becoming known and rolling out the patch.

A number of other measures could be developed.

Final remarks

The observations have shown that a reporting of vulnerabilities used by the state for active measures is likely to have only a minor effect on the increase in overall technical IT security. On the other hand, the value of the work of the security authorities is in many cases considered high, due to the high tactical enablement against potential malicious actors. The demand of some, that state authorities should refrain from proactively exploiting vulnerabilities for active measures therefore does not seem to make much sense; the net effect in security would be negative.

Nevertheless, processes can be introduced that allow a more precise assessment and an informed, accountable and cautious handling of offensively used vulnerabilities.

The DSI Industrial & Policy Recommendations (IPR) Series is published by the Digital Society Institute of ESMT Berlin, http://dsi.esmt.org.

DSI Industrial & Policy Recommendations (IPR) Series

Empfehlungen zur Organisation der Nutzung von Schwachstellen für staatliche Sicherheitszwecke

Sandro Gaycken (Digital Society Institute, ESMT Berlin)

Ausgabe 7, 2017

Wie kann das Problem modelliert werden?

Schwachstellen, auch bekannt als „Vulnerabilities“, „Bugs“ oder „Vulns“, sind strukturelle Fehler oder Programmierfehler, die von Hackern ausgenutzt werden können, um direkt Zugang zu den Systemen zu erhalten oder um Angriffe zu bauen, sogenannte „Exploits“.

Schwachstellen und Exploits haben in den letzten Jahren eine kritische Relevanz für staatliche Behörden im Sicherheitsbereich bekommen. Diese Behörden müssen im Kontext von Aufklärung, Forensik und Überwachung in der Lage sein, auf fremde Smartphones und Rechner zuzugreifen. Zwei Varianten dieses Zugriffs sind in Deutschland strategisch und politisch unerwünscht und weitgehend technisch oder regulativ ausgeschlossen: der gezielte Einbau von Schwachstellen als „Hintertüren“ in Technologieprodukte, rechtlich von den Herstellern erzwungen, und verdachtslose Massenüberwachung. Ein Einbau von Hintertüren ist vor allem strategisch unklug, da so das Vertrauen in deutsche Technologieprodukte im Exportmarkt stark beeinträchtigt würde und mit Exporteinbußen zu rechnen wäre. Massenüberwachung dagegen verstößt stark gegen historisch geprägte Vorstellungen zur Trennung staatlicher und privater Handlungsräume.

Eine mit beiden Einschränkungen verträgliche Vorgehensweise dagegen ist der gezielte Zugriff auf Rechner oder Smartphones durch das Hacken der Systeme. Der Autor hat dies in der Vergangenheit mehrfach als Lösungsweg empfohlen. Diese Vorgehensweise ist jedoch voraussetzungsreicher und schwieriger. Hohe Kompetenzen müssen angeschafft und vorgehalten werden, Schwachstellen haben oft nur begrenzte Lebensdauern, und Zugänge müssen oft manuell erhalten werden. Zudem muss die Vorsortierung von Verdächtigen und die Identifikation ihrer digitalen Geräte ohne Massenüberwachung über andere Wege erreicht werden. Über einen entschlossenen und breiten Anbau von Fähigkeiten, sowie über die Nutzung privater Exploit Reseller kann allerdings eine hinreichende Fähigkeit erreicht werden, die dann in höherem Maße konform ist mit deutschen strategischen und politischen Interessen.

Allerdings kann ein anderer möglicher Konflikt mit dieser Vorgehensweise diskutiert werden. Denn werden Schwachstellen entdeckt, werden diese in allen anderen Fällen an die Softwarehersteller gemeldet, damit diese sie beheben („Patchen“) können. So wird eine spätere oder weitere Nutzung der Schwachstellen durch Kriminelle oder andere Angreifer verhindert. Die für staatliche Zugriffe genutzten Schwachstellen müssen allerdings in den Produkten verbleiben, um für Überwachung, Forensik und Aufklärung genutzt werden können, so dass die staatlichen Behörden diese gerade nicht melden werden. So könnte eine höhere Unsicherheit an anderen Orten entstehen, indem Schwachstellen von Kriminellen genutzt werden, die staatlichen Behörden eigentlich bekannt sind und durch diese behoben werden könnten. Entsprechend entstehen in einigen Staaten erste Vorstellungen und Verfahren zu einer Beurteilung der möglichen Folgen des Nichtmeldens der von den Sicherheitsbehörden entdeckten Schwachstellen. In diesen Prozessen, in den USA etwa als „Vulnerability Equities Process“ bekannt, soll erwogen werden, ob der Wert der Nutzung einer Schwachstelle für Sicherheitsaufgaben gegenüber dem Risiko einer Ausnutzung der Schwachstelle durch kriminelle und andere Angreifer vertretbar ist oder ob das Risiko überwiegt, so dass die Schwachstelle eher gemeldet als genutzt werden sollte. Der Gewinn der Meldung einer Schwachstelle für ein Patching muss gegen den Gewinn ihrer Nutzung für staatliche Sicherheitsaufgaben abgewogen werden.

Dieses Papier will einige Analysen und Kommentare zu dieser Abwägungsfrage bieten.

Sollte ein Abwägungsprozess überhaupt formalisiert werden?

Erste Einsichten aus Dokumenten der Electronic Frontier Foundation zum amerikanischen „Vulnerability

Equities Process“ verraten nicht viel darüber, wie Abwägungsprozesse ablaufen. Es scheint jeweils eine Fall-zu-Fall-Entscheidung getroffen zu werden, in Teams von betroffenen oder verantwortlichen Einheiten. Der Entscheidungsprozess selbst ist nicht transparent, scheint aber von regionalen Regierungsmentalitäten geprägt zu sein. In den USA leiten etwa die Nachrichtendienste den Prozess, so dass ein Hauptgewicht auf der Ermöglichung staatlicher Fähigkeiten zu liegen scheint.

Da klare Verfahren und Kriterien aber derzeit noch nicht zu erkennen sind, wird die Entscheidung in den meisten Fällen ein politischer Aushandlungsprozess sein. Dieser unterliegt damit typischen politischen Dynamiken und wird je nach Anzahl der Beteiligten und Länge des Verfahrens in weiten Teilen schwer vorhersagbar oder nachvollziehbar sein. Einflüsse können durch darüber und darunterliegende politische Interessen, Macht- und Hierarchiegefüge, Fehlerkultur, Sicherheitskultur, Rotationsverfahren, besonders engagierte Einzelpersonen, Kooperationsinteressen, tagesaktuelle Presse, Oppositionsinteresse oder andere, ähnlich volatile Faktoren entstehen. Politisch geschultere und fähigere Entitäten werden zudem latent im Vorteil sein und ihre Interessen besser durchsetzen können.

Dieses informelle Verfahren hat den Vorteil, den betroffenen Akteuren breitere Handlungsspielräume einzuräumen, da prinzipiell auch außerhalb eines starren Rahmens liegende Argumente eingebracht werden können und da so auch auf Veränderungen im relevanten strategischen Anwendungsfeld besser reagiert werden kann. Allerdings besteht auch das Risiko schwerer Fehlentscheidungen, indem sich etwa weniger kompetente oder einseitig interessierte Entitäten mit in die eine oder andere Richtung - eher schädlichen Interessen allein aufgrund politischer Kompetenz durchsetzen. Zudem kann in dem aktuellen Prozess kaum Rechenschaft abgelegt und damit Verantwortlichkeit für Entscheidungen angebracht werden. Um Rechenschaftspflicht zu schaffen, wäre ein formaleres Verfahren mit konkreten, expliziten Entscheidungen auf Basis festgesetzter Listen von Spezifikationen und Anforderungen erforderlich.

Eine kluge Einrichtung würde eventuell ein semiformales Verfahren anstreben, in dem zwar feste Kriterien einer Bewertung durchgegangen werden müssen, ohne jedoch eine Entscheidung vorzuschreiben. So hätte die unter Umständen wichtige strategische Komponente ein politisches Vetorecht, ohne Verantwortlichkeit reduzieren zu können.

Was muss bewertet werden?

Wie oben erläutert muss in einem Abwägungsprozess der Gewinn der Meldung einer Schwachstelle für ein Patching gegen den Gewinn einer Nutzung dieser Schwachstelle für staatliche Sicherheitsaufgaben abgewogen werden. Konkreter ließe sich die Abwägung als „Kritikalität gegen Wert“ anstellen, indem die *Kritikalität* einer Schwachstelle für die individuelle und systemische Sicherheit der IT gegen den *Wert* dieser Schwachstelle für die Aufklärung von Verbrechen oder die operative nachrichtendienstliche oder militärische Nutzung erwogen wird.

Einfache Fälle wären Schwachstellen, in denen entweder Kritikalität sehr niedrig und Wert sehr hoch wären oder Kritikalität sehr hoch und Wert sehr niedrig. Solche Fälle werden aber nur selten eindeutig eintreten.

Allgemein lassen sich eine ganze Reihe von Kriterien anbringen, anhand derer Kritikalität und Wert evaluiert werden können.

Kritikalität:

- Zu erwartende CVSS Einstufung und die Gründe dafür
- Art und Verbreitung betroffener Systeme (Target Range)
- Ökonomische Kritikalität der Target Range
- Strategische Kritikalität der Target Range
- Mögliche strategische Effekte
- Mögliche systemische Effekte
- Sicherheits-Kritikalität der Target Range
- Einfachheit der Entwicklung von Exploits
- Mögliche technische Lokale der Wirkung
- Effektivität und Potential der Exploits
- Geschwindigkeit und Beschleunigung der Exploit-Entwicklung und der Exploit-Nutzung
- Nutzbarkeit als Stufe in modularen Angriffen
- Migrationspotential möglicher Exploits mit Weiterverbreitungsfunktionalitäten
- Mögliche Masseneffekte
- Vorhersagbarkeit von Wirkungen
- Mögliche direkte Schäden
- Mögliche indirekte Schäden
- Mögliche komplexe Effekte
- Mögliche Sicherheitsbeeinträchtigungen
- Common Case nach Akteursklassen
- Worst Case nach Akteursklassen
- Kosteneffizienz für Angreiferklassen
- Dual Use Aspekte
- Einfachheit der Detektion
- Einfachheit des Patching
- Kooperationsbereitschaft und -fähigkeit des Herstellers im Patching

Wert:

- Relevanz des Zugangs

- Bedarf des Zugangs
- Tiefe des Zugangs
- Einfachheit des Zugangs
- Nachhaltigkeit des Zugangs
- Risiko der Entdeckung des Zugangs
- Abstand zu relevanten Vulnerability Discovery Prozessen
- Erwartetes Shelf-Life des Exploits
- Einfachheit der Exploit-Entwicklung
- Eleganz des Exploits
- Erwartete Qualität des Exploits (z.B. Stabilität, Größe, Prozessgröße, Funktionalität, Tarnung, Breite der Plattformen, Interferenz mit anderen Apps, Agilität, Tunneling)
- Taktische Ermächtigung durch Exploit (z.B. Beständigkeit, Tarnung, Modularisierbarkeit, Eskalation & Elevation, Abfangen, Extraktion, Spurenkontrolle, Manipulation)
- Forensische Wertigkeit des Exploits
- Anzahl der Alternativen
- Vergleiche der Effektivität, Effizienz und Qualität von Alternativen
- Exklusivität

Viele weitere Punkte wären möglich, etwa indem klassische Risikobewertungen wie STRIDE querklassifiziert werden, wobei aber eine Neuausrichtung dieser eher eng technischen Kriterien mindestens auf systemische Effekte in der gesamten möglichen Target Range und auf Vergleichbarkeit stattfinden müsste.

Eine weitere wichtige Komponente der Abwägung liegt zwischen Kritikalität und Wert: die Möglichkeit der Sicherung der gefundenen Schwachstellen (OPSEC), so dass diese nicht gestohlen oder versehentlich oder absichtlich geleakt werden. Vor allem die Leaks der Shadowbroker oder Vault7 haben demonstriert, dass so eine erhebliche Veränderung des Gesamtrisikos und damit auch eine starke Veränderung des Abwägungsgewichts von Kritikalität und Wert entstehen kann. Auch hier können einige Charakteristiken abgefragt werden, deren Einschätzung zur Gesamtbetrachtung beitragen muss:

OPSEC:

- Bedingungen für die Einbehaltung
- Möglichkeit der phasenweisen Extraktion des Exploits
- Möglichkeit der operativen Kontrolle
- Mögliche Level der Cyber OPSEC
- Einfachheit der Detektion eines Missbrauchs
- Lokalisierbarkeit (Begrenzbarkeit) des Exploits
- Lokalisierbarkeit (Begrenzbarkeit) des Angriffs
- Mögliches Interesse dritter Parteien
- Nutzbarkeit für dritte Parteien
- Strategisches Risiko bei Verlust
- Risiko der Detektion laufender Tätigkeiten
- Risiko der Attribution
- Risiko der Nach-Attribution

Was für Probleme können im Abwägungsprozess entstehen?

Im Abwägungsprozess selbst können allerdings eine Reihe von Problemen entstehen.

Ein erstes Problem ist der Vergleich unterschiedlicher Kategorien. Bei einigen Schwachstellen können in der Betrachtung der Kritikalität nur monetäre Schäden und (meist eher hypothetische) Schäden an Privatheit angegeben werden, während in der Betrachtung des Wertes nicht selten Menschenleben die ausschlaggebende Basis bilden. Ein Beispiel sind Schwachstellen in Mobiltelefonen. Diese ermöglichen Kriminellen höchstens Erpressungen oder Störungen, während aber eine Nutzung durch Strafverfolger, Nachrichtendienste und Militärs erheblichen Wert bei der Aufklärung und Verhinderung von Gefahren für Leib und Leben hat. Aufgrund dieser Andersartigkeit der Kategorien werden bei der Bewertung politische Präferenzen nicht völlig auszuklammern sein.

Eine weitere Schwierigkeit bei der Abwägung besteht darin, dass die Bewertung hauptsächlich auf der taktischen Ebene stattfinden muss. Viele der anwendbaren Charakteristiken werden in ihrem realen oder möglichen Kontext betrachtet werden müssen, und dieser lässt sich sowohl für Kritikalität als auch für Wert nur auf der Ebene der Taktik festmachen. Taktische Ermächtigungen und mögliche taktische Wirkungen müssen primär identifiziert werden, um direkte und indirekte sowie strategische Schäden und Folgen betrachten zu können. Dies muss zudem komparativ zu anderen Varianten taktischer Verfahrensweisen geschehen. Wenn etwa eine bestimmte Schwachstelle einen taktischen Zugang ermöglicht, der durch seine exotische Position für einen Dienst gut nutzbar ist, die gleiche Taktik aber für Kriminelle mit bereits deutlich günstigeren Methoden durchgeführt werden kann, ist eine Kritikalität weniger wahrscheinlich, während der Wert höher ist.

Das größere Problem bei der Bewertung der taktischen Ebene ist allerdings der Mangel an Analysen dieser Ebene. Zumeist sind Taktiken nur denjenigen bekannt, die operativ damit tätig sind, offensiv wie defensiv, so dass ein großer Teil unter hohe Geheimhaltung fällt. Selbst dort ist aber das Wissen zur Bewertung von Taktiken noch meist stark unterentwickelt und lückenhaft. Zudem sind Taktiken oft von stark veränder-

lichen Faktoren abhängig, so dass eine Bewertung immer auf einem aktuellen Niveau getroffen und gehalten werden muss.

Führt das Melden von Schwachstellen überhaupt zu einer Erhöhung der IT-Sicherheit?

Für viele Schwachstellen, die zwischen den beiden Extremen „eindeutig kritisch“ oder „eindeutig hochwertig“ liegen, kann ein weiteres interessantes Problem betrachtet werden, dem etwas mehr Raum in der Diskussion gegeben werden muss: der Einfluss auf die systemische Sicherheit. Es kann nämlich auf Seiten der Kritikalität nicht genau gesagt werden, ob das Melden und Patchen von Sicherheitslücken überhaupt einen signifikanten Härtungseffekt auf die dahinterliegende IT-Landschaft hat, ob also das vereinzelte Patchen von Schwachstellen zu einer echten Reifung der Sicherheit führt oder nicht.

Ein erster Zweifel darf allein aufgrund der Anzahl von Schwachstellen angemeldet werden. Während es für einige Bereiche wie das iOS, den Android Kernel oder einige TrustZone Umsetzungen deutlich schwerer geworden ist, in ihrer Struktur bekannte Schwachstellen zu finden, sind in anderen Bereichen wie Betriebssystemen und den meisten Anwendungen immer noch viele hundert bis viele tausend Schwachstellen anzunehmen, in den meisten Anwendungen anteilsproportional noch deutlich mehr. Diese Zahlen werden sich zudem durch hinzukommende Neuentwicklungen, insbesondere im aktuellen Digitalisierungswahn, über die Zeit konstant vergrößern und nicht in Richtung einer Sicherheitsreife verringern. Des Weiteren hat nach gängigen Statistiken in der Office-IT etwa ein Drittel davon eine erhöhte CVSS-Kritikalität, in der Industrial-IT etwa die Hälfte.
Wenn folglich in einem normalen IT-Basisprodukt nicht nur einige Dutzend, sondern konstant viele tausend kritische Schwachstellen vorhanden sind und wenn die Entwicklungsprozesse ohnehin eher mehr als weniger Schwachstellen einbringen müssen, kann argumentiert werden, dass das Melden einzelner Schwachstellen selbst bei einer hohen Kritikalität keine nennenswerte oder nachhaltige Gesamterhöhung der Sicherheit leisten wird. Fähige und motivierte Angreifer werden ohnehin eine kritische Schwachstelle finden, wenn sie gezielt und methodisch suchen, und die meisten staatlichen Behörden benötigen pro System ohnehin nur einige wenige Schwachstellen. Dies beeinflusst also nachhaltig das Verhältnis zwischen Kritikalität und Wert, da selbst bei der Meldung der meisten kritischen Schwachstellen keine signifikante Erhöhung der Gesamtsicherheit zu erwarten ist, während aber der Wert der Schwachstellen sofort vollständig kollabiert.

Leider ist aber die Faktenlage für eine präzise Einschätzung des systemischen Sicherheitseffekts ungemein schwach. Es sind keine exakten Messungen oder auch nur gut informierte Abschätzungen verfügbar, so dass nur Schätzungen auf der Basis der wenigen bekannten Defektraten und auf Erfahrungswerten der Hacking-Community unternommen werden können. Die Schwere des Entdeckens von Schwachstellen, die sich etwa in den Graumarktpreisen der Exploits abbildet, kann allerdings nur begrenzt als Maßstab betrachtet werden, da diese noch von einer Reihe anderer Faktoren maßgeblich beeinflusst werden, wie etwa vorhandene Tools, vorhandenes Knowhow, erforderliche Ressourcen, notwendige Fachkenntnisse, sowie Art des Bedarfs, so dass dort zwar qualitative Relationen, aber kein direktes Verhältnis abgelesen werden darf.

Wie würde sich ein neues Schwachstellenregime auf Akteure ausprägen?

Eine weitere wichtige Frage ist, ob bei einer expliziten gesetzlichen Regulierung der Abwägung überhaupt mehr Schwachstellen gemeldet würden. Dies kann beurteilt werden, wenn bedacht wird, wie die Akteure ihr Verhalten bei einer expliziten Regulierung voraussichtlich ändern würden.
Die nachrichtendienstlichen, kriminalistischen und militärischen Akteure, die Schwachstellen für Offensivzwecke suchen, stehen in allen Ländern ohne Ausnahme unter hohem finanziellen und Leistungsdruck. Im Bereich „Hacking“ haben zudem beinahe alle kaum nennenswerte Kompetenzen aufbauen können, so dass nur wenig gutes Personal überhaupt zur Verfügung steht. In vielen, selbst großen Industrieländern sind das oft nicht mehr als ein bis einige Dutzend Personen. Folglich werden diese Akteure diese stark beschränkten und dringend benötigten Ressourcen nicht in das Aufdecken von Schwachstellen stecken wollen, die ihnen nicht garantiert zugutekommen. Sie werden einen Prozess der vorangehenden Bewertung einrichten, der vor dem Prozess der Entdeckung prüfen wird, welche Schwachstellen in welchem Bereich und in welcher Kritikalität entdeckt werden dürfen und welche abgegeben werden müssten, so dass nur an denen gearbeitet wird, die auch genutzt werden können. Damit ist nicht zu erwarten, dass aus diesen Institutionen überhaupt noch Schwachstellen gemeldet werden. Im Vergleich zur aktuellen Situation entstünde also eher ein Nettoverlust in der Meldung von Schwachstellen. Aktuell werden immerhin in einigen Fällen kritische Schwachstellen gemeldet, da der Entdeckungsprozess eben nicht auf eine Meldepflicht hin vorstrukturiert ist.

Regierungsstellen könnten noch eine andere Rolle spielen. Eine stärker aktive Regulierungsoption wäre es, eine eigene Regierungsinstitution einzusetzen, die Schwachstellen entdeckt und der Softwareindustrie mitteilt. Allerdings hätte diese Regierungsstelle mit hoher Konkurrenz um die dafür verfügbaren Talente zu rechnen, bei einer gleichzeitig deutlich langweiligeren

Aufgabe, und damit kaum Chancen, einen nennenswerten kompetenten Personalstamm aufzubauen. Unter normalen Gehalts- und Arbeitsbedingungen werden sich kaum mehr als zehn bis zwanzig Personen finden lassen, die in der Lage sind, in großen und bereits nachgehärteten Legacy-Systemen in manueller Code-Analyse oberhalb der Qualität technischer Analysetools Schwachstellen zu finden. Lediglich in kleineren Spezialbereichen, in denen besonderes Fachwissen angeworben werden kann und in denen normale Analysetools nicht greifen, wie einige Felder der Industrial IT, könnte dies gelingen. Zudem würde eine solche staatlich finanzierte Stelle sich dem berechtigten Vorwurf aussetzen, eine teure und umständliche Aufgabe der IT-Industrie zu übernehmen, die auf diesem Wege eigene, durch Nachlässigkeit in der Qualitätssicherung entstandene Kosten ungerechtfertigter Weise in hohe Gemeinkosten verwandeln kann.

Ein weiterer Akteur, der sein Verhalten ändern würde, wäre der Graumarkt der Exploit-Reseller und der auf freier Basis für Regierungsstellen arbeitenden Hacker. Diese würden nur noch mit großer Vorsicht an Regierungen verkaufen, die einen Veröffentlichungsprozess haben, sofern nicht explizit zugesichert werden kann, dass die angekaufte Schwachstelle oder der angekaufte Exploit nicht veröffentlicht werden, oder sie würden nur zu Exklusivpreisen verkaufen, die im Schnitt das zwei- bis dreifache der normalen Preise sind. Auch dann könnten einige Anbieter allerdings eher zurückhaltend sein, da eine Veröffentlichung der Schwachstelle dem Hersteller häufig auch Rückschlüsse auf Methoden oder Perspektiven des Hackers liefert, so dass das Handlungspotential des Anbieters und damit der Marktwert auch grundlegender geschwächt werden.

Eine Variante dieses Akteurs sind Hacker, die Bug Bountys kassieren, indem sie Schwachstellen der Softwareindustrie direkt melden und diese nicht im Graumarkt verkaufen, weil der Wert dort unterhalb des Bountys liegen würde oder weil ihnen der Graumarkt unheimlich oder nicht zugänglich ist. Diese Hacker spielen gegenwärtig ohnehin nur eine eher untergeordnete Rolle, da der Graumarkt viele deutlich stärker anzieht als Bug Bounty Programme, und sie würden ohnehin nur dann ihr Verhalten ändern und Schwachstellen an Staaten mit Meldeprozessen weitergeben, wenn dort ein Bounty mit höherem Wert angeboten würde oder wenn sie vom Verhalten der Softwareindustrie konkret oder allgemein enttäuscht sind. Dies wird nur für eine geringe Zahl eher weniger relevanter Schwachstellen gelten.

Ebenfalls ihr Verhalten kaum ändern werden andere Firmen, die routinemäßig Schwachstellen der bei ihnen laufenden oder von ihnen verbauten Software an die Hersteller melden. Hier bestehen etablierte Prozesse, die von einem staatlichen Meldeprozess voraussichtlich nicht beeinträchtigt werden, zumindest solange die Schwachstellen auch gepatcht werden und solange staatliche Stellen nicht eigene, höhere Bountys anbieten.

Für Softwarehersteller könnten sich einige Implikationen ergeben, die aber gegenwärtig noch schwer abzuschätzen sind, da die Modalitäten der Kooperation erst zu klären wären. Wenn sehr viele Staaten Schwachstellen melden, entstehen allerdings viele Gelegenheiten, weil die Fähigkeiten der Hersteller zu Patchen ohnehin schon am Kapazitätsende sind.

Sollten Exploits angekauft werden, um sie zu veröffentlichen?

Die Idee, dass staatliche Stellen teure Schwachstellen aus dem Graumarkt ankaufen, um sie zu melden, klingt zunächst absurd. Die so verfahrenden Staaten würden damit die Bug Bounty Programme der Softwareindustrie parallelisieren und aufgrund der deutlich höheren Preisen mittelfristig faktisch unterwandern und abtöten. Allerdings wurden entsprechende Gedanken tatsächlich angestellt. Die Bundesregierung hat in einigen Fällen bereits Schwachstellen am BSI angeboten bekommen, bei denen überlegt wurde, wie damit zu verfahren sein. Hier entsteht rechtlich die interessante Frage, ob mit einem gesetzlich formalisierten Prozess der Meldung eine Verpflichtung zum Ankauf solcher Schwachstellen entsteht, was wiederum eine vermutlich ungünstige Entwicklung nach sich ziehen könnte. Ein eigener Graumarkt könnte entstehen, spezifisch für die von Staaten als kritisch angesehenen Schwachstellen, mit einer eher hochpreisigen Struktur und zum „Nachteil“ der Bug Bounty Programme der Softwareindustrie, die damit erneut eigene Kosten in Gemeinkosten umwandeln könnten.

Was sind mögliche globale strategische Konsequenzen?

Ein weiteres Element, das sich bei einer Einrichtung eines Abwägungsprozesses ausprägen kann, sind internationale strategische Folgen für die entstehende Asymmetrie zwischen Ländern ohne eine entsprechende Regulierung und Ländern mit einer solchen Regulierung. Staaten ohne Veröffentlichungsprozess werden rücksichtsloser Schwachstellen finden und Exploits entwickeln können. Sie werden schneller sein, da sie keine Reviews durchlaufen müssen, da sie auch einfach zu findende Schwachstellen nutzen können und da sie eine breitere Palette an Talenten nutzen können. Sie werden voraussichtlich auch ein beliebterer Kunde im Exploit-Graumarkt sein.

Als Folge dieser Vorteile in Entwicklung und Beschaffung werden sie in ihren militärischen und nachrichtendienstlichen Cyberoperationen taktisch deutlich flexibler und agiler sein, da sich ihnen mehr Optionen bieten und da eine andere und breitere taktische Kombinatorik

genutzt werden kann. Da keine Target Ranges kategorisch ausgeschlossen werden dürften, wird auch die Auswahl möglicher strategischer Optionen deutlich breiter sein und entsprechende Akteure könnten in vielen Feldern arbeiten, die anderen nicht zugänglich sind. Zudem werden über die Zeit nicht nur die Arsenale, sondern auch die Fähigkeiten der Operateure deutlich besser als jene von Staaten mit einer starken Regulierung von Schwachstellenmeldungen.

Da weiter davon auszugehen ist, dass vor allem Staaten ohne starke Zivilgesellschaft, Demokratie und Rechtsstaat oder Staaten in härteren Konfliktsituationen auf einen Veröffentlichungsprozess verzichten und die asymmetrischen Vorteile eines strengeren Schwachstellenregimes in anderen Ländern auch gezielt ausnutzen werden, kann eine weitere Folge eine asymmetrische offensive Ermächtigung autoritärer Staaten sein.

Wie kann der Prozess staatlicher Exploit-Entwicklung sicherer gestaltet werden?

Es bestehen eine Reihe von Optionen, um die staatliche Entwicklung von Hackerangriffen sicherer zu machen und das Verhältnis von Kritikalität und Wert zu verbessern. Zum einen sollten beide Merkmale bei Einkauf und Entwicklung oder Customization von Exploits betrachtet werden. Zum anderen müssen alle möglichen Verfahren für eine sehr hohe OPSEC identifiziert und rigoros umgesetzt werden.

Schließlich bleibt eine Reihe weiterer Optionen, die Risiken für die Allgemeinheit minimieren.

Etwa können die offensiven staatlichen Stellen eher hochwertige und exotische Exploits und Schwachstellen entwickeln und ankaufen. Bei diesen ist es weniger wahrscheinlich, dass sie von Kriminellen oder anderen, weniger talentierten Gegnern entdeckt werden, so dass auch das Risiko der Folgen eines Nicht-Meldens direkt proportional sinkt. In dieser Richtung kann eine umfassendere Methodologie entwickelt werden, da sich hochwertige und exotische Exploits glücklicherweise als Kategorien noch gut erfassen lassen und da entsprechende Fähigkeiten bei Entwicklern und bei Verkäufern gut identifiziert werden können, eine hohe eigene Kompetenz in diesem Feld vorausgesetzt.

Offensive staatliche Stellen könnten sich zudem bemühen, zu erkennen, ob die von ihnen genutzten Schwachstellen von Gegnern entdeckt wurden und genutzt werden. Es könnten schwachstellenspezifische Indikatoren entwickelt werden, nach denen folgend laufende Angriffe oder sogar potentielle Angriffe analysiert werden können. Werden Angriffe identifiziert, bei denen die eigene genutzte Schwachstelle involviert sein könnte, kann die IT-Industrie entsprechend informiert werden.

Schließlich können offensiv agierende staatliche Stellen für die eigenen Schwachstellen umfangreiche Dokumentationen erstellen und erste Entwicklungen für Patches vornehmen, soweit extern möglich. Bei Bekanntwerden der Schwachstelle kann dieses Wissen sofort der IT-Industrie mitgeteilt werden, und es kann beim Patching assistiert werden, um die Phase zwischen Bekanntwerden einer Schwachstelle und Ausrollen des Patches deutlich zu verkürzen.

Einige weitere Maßnahmen ließen sich entwickeln.

Abschließende Bemerkungen

Die Betrachtungen haben gezeigt, dass eine Veröffentlichung staatlich genutzter Schwachstellen vermutlich nur einen geringen Effekt auf die Erhöhung der technischen IT-Sicherheit haben dürften, während auf der anderen Seite der Wert für die Arbeit der Sicherheitsbehörden in vielen Fällen aufgrund der hohen taktischen Ermächtigung gegen mögliche Gegner als hoch anzusehen ist. Der von verschiedenen Stellen geforderte Verzicht auf die offensive staatliche Nutzung von Schwachstellen scheint daher unsinnig, der Gesamtsicherheitseffekt wäre negativ.

Dennoch können Prozesse eingeführt werden, die eine präzisere Abwägung und einen gegenüber möglichen Kollateral- oder Dual Use-Schäden informierten und vorsichtigen Umgang mit offensiv genutzten Schwachstellen ermöglichen. So kann auch eine bessere Verantwortlichkeit in den Prozessen verankert werden.

Die DSI Industrial & Policy Recommendations (IPR) Series wird herausgegeben vom Digital Society Institute der ESMT Berlin, http://dsi.esmt.org.