DSI | DIGITAL SOCIETY INSTITUTE BERLIN

ESMT BERLIN

DSI Industrial & Policy Recommendations (IPR) Series

Vulnerabilities in IT-security products

Sandro Gaycken (Digital Society Institute, ESMT Berlin)

Issue 1, 2017

In October 2016, the Digital Society Institute hosted a workshop dedicated to the topic of vulnerabilities at large and in particular of vulnerabilities in security products. The workshop included talks from Thomas Dullien (former Google Project Zero), Matthias Luft (ERNW), Dr. Christoph Peylo (T-Labs), and a comment from Michael Kranawetter (Head of Information Security Microsoft Germany).

1. The facts

As the workshop participants identified, IT-security products commonly suffer from security issues. As their basic paradigms haven't evolved significantly from signature-based detection, they have to do a lot of parsing, perform many different tasks on different processes, in turn generating a high internal complexity and a high number of weaknesses, gaps and vulnerabilities in code and processes. Defect rates can be much higher than in other software products and persistent, as the IT-sec industry is still dominated by SMEs, who are not able to invest into expensive procedures for software quality assurance or verification.

Most security products also lack basic security features in themselves, examples including ASLR (Address Space Layout Randomization) or sandboxing, and run in privileged mode with high levels of access across the systems they are supposed to protect. Many of these issues are well known throughout the industry, but not tackled as solutions are deemed too costly and as the uninformed market doesn't demand them. Sadly, the market rather rewards fancy slideshows and interfaces, so money is put into marketing rather than quality assurance. Much of the actual innovation effort is devoted to keeping pace with the race of innovations in the underlying systems to be protected, so the security products can deliver their functions in a constantly changing environment. Given the high defect rates, the bad coding and quality assurance practices, and the lack of basic security features while running on high privileges in the system, IT-security products are attractive and willing targets for attackers. The workshop group deemed it likely that any system expecting mid-level or targeted attacks will suffer a net loss in security, if IT-security products are implemented.

Creating transparency for the security of IT-security products is a demanding task. Objective, scientifically valid methods to assess the security quality of the products do not exist, nor is there an entity conducting such assessments. Pen testing usually doesn't include a test of the security environment as an attack surface, and reverse engineering IT-security products is mostly illegal as it violates the EULA and is not easy for security testers as higher-end security products are very expensive. In addition, there is no tolerance in the IT-security market for an open discourse about the weaknesses and vulnerabilities of IT-security products. Publications of tests are usually met with law suits and immediate demands to withdraw all publicized material, as has just happened in the case of the FireEye-hack "Playing with Fire".

Certifying security products could be an option, but certification processes are much too slow to warrant competitive advantage through certification. These highly bureaucratic processes take around two years, despite the group deemed it entirely possible to conduct the necessary assessments within three weeks. In this speed, products are outdated when they are finally certified.

2. Conclusion

Ironically, implementing IT-security products can be dangerous and create a net loss in security, as many of the products are highly vulnerable and open critical attack vectors into the systems they are supposed to protect. This would not have to be the case. Many basic security measures could be applied. But the relevance of security in security is not a topic yet and the according characteristics are not transparent or measurable, so the market does not demand security in security yet.

In order to improve this situation, both short-term and long-term, the workshop members and the DSI have developed a set of recommendations.

3. Recommendations

Recommendations for industry

Demand security characteristics

Before striking a contract with a security firm, demand to see everything that is being done to secure the product itself. Ask for defect rates, quality assurance processes, penetration tests, technical security quality features such as ASLR or sandboxes, practices in reporting and disclosure, security policies and for the amount and quality of personnel solely assigned to assuring security in security products. A guide to such questions can be found in the DSI study on "Cyber-readiness for small and medium enterprises".

Establish more neutral and critical expertise

Neutral and critical experts are often not included in critical decision-making processes on security and are frequently not invited to larger industrial or political conferences to avoid confrontation. But critical confrontation must be included, not excluded, to improve security.

Create third party bug bounty programs

Industrial IT-users should offer bug bounties for vulnerabilities and security issues in IT-security products. To enable this activity, they should request permissions for white box testing of IT-security products when contracting such a product. A procedure will have to be defined to warrant the confidential treatment of source code for third parties. Industrial IT-users should consider sponsoring IT-security products to small hacking companies for testing.

Demand cooperation in vulnerability management

IT-security customers must demand by contract proper vulnerability and patching management processes from IT-security companies and assistance in vulnerability management, in patching and during incidents related to the IT-security product.

Create information and information sharing on security of IT-security

Industrial IT-users should generate information on security issues in security products. Systematic tests could be designed and conducted by a joint center for testing. Academic institutions or industrial initiatives could conduct such testing, similar to Google's Project Zero, but any testing would have to follow a rigid methodology and involve high talent to be effective. Test results could be published. In addition, industrial IT-users should create larger peers groups to exchange knowledge about vulnerabilities in IT-security products and form regimes to generate more pressure on IT-security companies to improve the security quality of their products.

Recommendations for policy

Basic security measures must be mandatory

Wherever regulators require a specific level of IT-security, they must define and demand basic security functionalities within security products, levels of code quality and tolerance levels for code defect rates. Sandboxing is an example of a comparatively inexpensive technology with significant impact on product security. If security-wise critical design choices are being made such as the software running on high privileges, functional reasons and risk assessments must be provided.

Security of security must be transparent

Security quality must be tested and rendered comparative, so the market can develop along objective characteristics. Security measures and policies, vulnerabilities and any management processes affecting software quality, vulnerability and patch management must be publicized. Claims to security must be tested methodologically to be verified. Results must be published. IT-security agencies should use their rights to testing IT products with an emphasis on security products.

EULAs must enable reverse engineering

Independent tests of the security of IT-security, whether academic or by IT-users, must be legal. To legalize such tests, EULAs should not forbid reverse engineering, but enable and describe a cooperative process of responsible reverse engineering. Contradictory copyright regulation should be modified.

Legal protection for responsible disclosure procedures

As many IT-security companies still react aggressively upon the disclosure of their weaknesses, such disclosure, if responsible, must be protected by law. If the disclosure of a weakness is in the public interest, the researcher and publisher should not be liable.

Review IT certification processes

The certification process for good IT-security products must be reformed. It must be possible to certify a product, if necessary preliminarily, within one month. Otherwise, certification will be ever less relevant for actual market dynamics.

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

DSI | DIGITAL SOCIETY INSTITUTE BERLIN

ESMT BERLIN

DSI Industrial & Policy Recommendations (IPR) Series

Vulnerabilities in IT-Sicherheitsprodukten

Sandro Gaycken (Digital Society Institute, ESMT Berlin)

Ausgabe 1, 2017

Im Oktober 2016 veranstaltete das Digital Society Institute einen Workshop zu Schwachstellen von IT-Sicherheitsprodukten. Der Workshop beinhaltete Vorträge von Thomas Dullien (ehemals Google Project Zero), Matthias Luft (ERNW), Dr. Christoph Peylo (T-Labs) und einen Kommentar von Michael Kranawetter (Head of Information Security Microsoft Deutschland).

1. Gegenwärtiger Stand bei Schwachstellen von IT-Sicherheitsprodukten

IT-Sicherheitsprodukte haben häufig Sicherheitsprobleme. Da sich die grundlegenden technischen Ansätze meist nicht deutlich aus der signaturbasierten Erkennung heraus weiterentwickelt haben, müssen IT-Sicherheitsprodukte viele unterschiedliche Prozesse beherrschen und beobachten, was zu einer hohen Komplexität der Produkte selbst und der technischen Verfahren führt. Diese hohe Komplexität führt ihrerseits zu funktionalen Lücken und Sicherheitsschwachstellen durch fehlerhaften Code. Defektraten in solchen Produkten können sehr viel höher sein als bei anderen Softwareprodukten und lange unentdeckt bleiben, da die IT-Sicherheitsbranche von KMU dominiert wird, die nicht in der Lage sind, in teure Verfahren zur Qualitätssicherung oder Überprüfung der Software zu investieren.

Die meisten Sicherheitsprodukte weisen keine grundlegenden inneren Sicherheitsmerkmale, z.B. ASLR (Address Space Layout Randomization) oder Sandboxing auf. Sie werden in der Regel im privilegierten Modus ausgeführt und haben weitgehenden Zugriff auf die Systeme, die sie schützen sollen. Viele dieser Probleme sind in der Industrie bekannt, werden aber nicht angegangen, da ihre Lösung als zu teuer betrachtet wird und der Markt sie nicht fordert, da dieser meist nicht in der Lage ist, die Sicherheit von Sicherheit adäquat zu beurteilen, so dass sich eher ausgefallene Präsentationen und Benutzeroberflächen durchsetzen als harte funktionale Merkmale. Geld wird eher in Marketing gesteckt als in Qualitätssicherung. Ein Großteil der tatsächlichen Produktinnovation erfolgt allein, um mit der Innovation der zu schützenden Systeme Schritt zu halten, um in dem sich ständig verändernden Umfeld ihre Funktionen weiterhin liefern zu können.

Angesichts der hohen Defektraten, der schlechten Programmierung und Qualitätssicherung, sowie dem Fehlen grundlegender Sicherheitsfunktionen bei gleichzeitig hohen Privilegien sind IT-Sicherheitsprodukte bei ihrer Ausführung im System attraktive Ziele für Angreifer. Vor dem Hintergrund dieser Analyse ist es sehr wahrscheinlich, dass Systeme, die das Ziel fortgeschrittener oder gezielter Angriffe sind, durch den Einsatz von IT-Sicherheitsprodukten keinen Gewinn, sondern netto sogar einen Verlust an Sicherheit erleiden.

Die Schaffung von Transparenz über die Sicherheit von IT-Sicherheitsprodukten ist eine anspruchsvolle Aufgabe. Objektive, wissenschaftlich valide Methoden zur Bewertung der Sicherheitsqualität der Produkte sind nicht vorhanden. Es gibt auch keine Institution, die solche Beurteilungen durchführt. Penetrationstests beinhalten in der Regel keinen Test der

IT-Sicherheitsumgebung als Angriffsziel. Reverse Engineering von IT-Sicherheitsprodukten ist meist illegal, da es in der Regel gegen die Endnutzer-Lizenzbestimmungen (EULA) verstößt. Reverse Engineering ist zudem für IT-Sicherheitstester nicht einfach, da hochwertige Sicherheitsprodukte sehr teuer sind. Darüber hinaus gibt es im IT-Sicherheitsmarkt keine

Toleranz für einen offenen Diskurs über die Schwächen und Schwachstellen von IT-Sicherheitsprodukten. Der Veröffentlichung von Tests folgen in der Regel Rechtsstreitigkeiten und unmittelbare Forderungen, die publizierten Materialien zurückzuziehen, wie es gerade im Fall des FireEye-Hacks „Playing with Fire“ geschehen ist.

Die Zertifizierung von Sicherheitsprodukten könnte eine Option sein. Zertifizierungsprozesse sind aber zu langsam, um durch sie Wettbewerbsvorteile zu erringen. Die höchst bürokratischen Zertifizierungsprozesse dauern etwa zwei Jahre, obwohl es leicht möglich wäre, die notwendigen materiellen Beurteilungen innerhalb von drei Wochen durchzuführen. Mit dieser heutigen Geschwindigkeit des Zertifizierungsprozesses sind Produkte oft bereits veraltet, wenn sie zertifiziert sind.

2. Schlussfolgerung

Die Implementierung von IT-Sicherheitsprodukten kann paradoxerweise gefährlich sein und einen Nettoverlust an Sicherheit verursachen, da viele der Produkte anfällig sind und kritische Angriffs-Vektoren in den Systemen öffnen, die sie schützen sollen. Das muss nicht notwendigerweise so sein. Viele grundlegende Sicherheitsmaßnahmen könnten auch für IT-Sicherheitsprodukte angewendet werden, Qualitätssicherungsprozesse wie Secure Development Lifecycles könnten und müssten sogar in besonders hohem Maße angewendet werden. „Sicherheit der IT-Sicherheit“ ist jedoch derzeit noch kein Thema. Entsprechende Sicherheitseigenschaften von IT-Sicherheitsprodukten sind nicht transparent oder nicht messbar, so dass der Markt noch keine Sicherheit der IT-Sicherheit nachfragt.

Zur Verbesserung dieser Situation haben die Teilnehmer des Workshops und das DSI eine Reihe von Empfehlungen entwickelt.

3. Empfehlungen

Empfehlungen an die Industrie

Fragen Sie Sicherheitsmerkmale nach

Bevor Sie einen Vertrag mit einer Sicherheitsfirma schließen, fragen Sie gezielt nach Maßnahmen, um das Produkt selbst zu sichern. Fragen Sie nach Defektraten, Qualitätssicherungsprozessen, Penetrationstests, technischen Sicherheitsmerkmalen wie ASLR oder Sandboxing, nach Praktiken in der Berichterstattung und Offenlegung von Schwachstellen, nach Sicherheitsrichtlinien und der Menge und Qualität des Personals, das ausschließlich der Sicherung von IT-Sicherheitsprodukten zugewiesen ist. Ein Leitfaden zu solchen Fragen findet sich in der DSI-Studie „Cyber-readiness for Small and Medium Enterprises“.

Entwickeln Sie neutrale und kritische Expertise

Neutrale und kritische Experten sind oft nicht in relevanten Entscheidungsprozessen zur Sicherheit einbezogen und häufig nicht zu größeren industriellen oder politischen Konferenzen eingeladen, um Konfrontationen zu vermeiden. Kritische Expertise sollte einbezogen werden, um die Sicherheit der Produkte zu verbessern.

Erstellen Sie Bug-Bounty-Programme für außenstehende Dritte

Industrielle IT-Anwender sollten Prämien für das Finden von Schwachstellen und Fehlfunktionen in IT-Sicherheitsprodukten anbieten. Um das zu ermöglichen, sollten sie Berechtigungen für White-Box-Tests von IT-Sicherheitsprodukten bei der Beschaffung solcher Produkte einfordern. Ein Verfahren muss definiert werden, um die vertrauliche Behandlung von Quellcodes durch Dritte sicherzustellen. Industrielle IT-Anwender sollten das Bereitstellen von IT-Sicherheitsprodukten für kleine Hacking-Unternehmen zwecks Prüfung erwägen.

Fordern Sie vom Hersteller eine Zusammenarbeit im Vulnerability Management ein

IT-Sicherheitskunden müssen von den IT-Sicherheitsunternehmen eine vertragliche Zusicherung von ordnungsgemäßen Vulnerability- und Patching-Management-Prozessen einfordern. Sie sollten zudem Unterstützung beim Schwachstellenmanagement, beim

Patching und bei Vorfällen im Zusammenhang mit dem IT-Sicherheitsprodukt vertraglich vereinbaren.

Stellen Sie Informationen bereit und ermöglichen Sie den Informationsaustausch über die Sicherheit der IT-Sicherheit

Industrielle IT-Anwender sollten Informationen über Sicherheitsprobleme in IT-Sicherheitsprodukten aufbereiten. Systematische Untersuchungen könnten von gemeinsamen Testzentren entworfen und durchgeführt werden. Akademische Einrichtungen oder industrielle Initiativen könnten solche Tests durchführen, ähnlich wie Googles Project Zero. Alle Tests müssen einer festgelegten Methodik folgen und benötigen höchste Fachqualifikation, um wirksam zu sein. Testergebnisse sollten veröffentlicht werden. Darüber hinaus sollten industrielle IT-Anwender größere Peer-Gruppen für den Wissensaustausch über Schwachstellen in IT-Sicherheitsprodukten aufbauen und Verfahrensweisen entwickeln, die mehr Druck auf IT-Sicherheitsunternehmen ausüben, damit diese die Sicherheitsqualität ihrer Produkte erhöhen.

Empfehlungen an die Politik

Grundlegende Sicherheitsmaßnahmen müssen obligatorisch sein

Überall dort, wo Behörden durch Vorschriften ein bestimmtes Niveau an IT-Sicherheit festlegen, müssen sie grundlegende Sicherheitsfunktionalitäten innerhalb der IT-Sicherheitsprodukte, ein hohes Niveau an Qualität des Codes sowie eine Toleranzgrenze für Fehlerraten im Code definieren und einfordern. Sandboxing ist ein Beispiel einer vergleichsweise kostengünstigen Technologie mit erheblichen Potentialen für die Produktsicherheit. Wenn sicherheitskritische Entscheidungen über das Design getroffen werden, z.B. dass die Software mit hohen Privilegien ausgeführt wird, dann müssen funktionale Gründe und Risikobewertungen dargelegt werden.

Sicherheit der IT-Sicherheit muss transparent sein

Die Qualität der IT-Sicherheitsprodukte muss transparent geprüft und bereitgestellt werden, so dass sich der Markt anhand objektiver Merkmale entwickeln kann. Sicherheitsmaßnahmen und Richtlinien, Schwachstellen und alle Verwaltungsprozesse, die die Qualität der Software beeinflussen, müssen veröffentlicht werden. Sicherheitsaussagen der Produkte sollten nur nach vorheriger methodischer Prüfung veröffentlicht werden. IT-Sicherheitsbehörden sollten ihre Rechte zur Prüfung von IT-Produkten nutzen und einen Schwerpunkt auf IT-Sicherheitsprodukte legen.

EULAs müssen Reverse Engineering ermöglichen

Unabhängige Tests der Sicherheit der IT-Sicherheit, ob akademisch oder durch IT-Nutzer, müssen legal sein. Um solche Tests zu erlauben, sollten EULAs Reverse Engineering nicht verbieten, sondern einen kooperativen Prozess des verantwortlichen Reverse Engineering ermöglichen und beschreiben. Entgegenstehende Urheberrechtsvorschriften sollten geändert werden.

Rechtsschutz für verantwortungsvolle Offenlegungsverfahren

Da viele IT-Sicherheitsunternehmen immer noch aggressiv auf die Offenlegung ihrer Schwächen reagieren, muss eine solche Offenlegung, wenn sie verantwortungsvoll geschieht, gesetzlich geschützt werden. Wenn die Offenlegung einer Schwäche im öffentlichen Interesse liegt, sollten Forscher und Herausgeber nicht haftbar gemacht werden können für die Veröffentlichung.

Reform des IT-Zertifizierungsverfahren

Der Zertifizierungsprozess für gute IT-Sicherheitsprodukte muss reformiert werden. Es muss möglich sein, ein Produkt, gegebenenfalls vorläufig, innerhalb eines Monats zu zertifizieren. Andernfalls wird die Zertifizierung für die tatsächliche Marktdynamik immer weniger relevant sein.

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