Bundesamt
für Sicherheit in der
Informationstechnik

SENSIBILISIERUNG

Lebenszyklus einer Schwachstelle

„Nach Bekanntwerden einer neuen Zero-Day-Schwachstelle hat der Hersteller ein Advisory veröffentlicht, in dem bis zur Fertigstellung eines Patches ein Workaround für betroffene Systeme beschrieben ist“. So oder so ähnlich lauten oft die Mitteilungen der IT-Abteilungen oder die Presseberichte, in denen von einer neuen Software-Schwachstelle die Rede ist. Schwachstellen in Software-Produkten sind eine der wesentlichen Ursachen für IT-Sicherheitsvorfälle. Die folgende Analyse beschreibt den „Lebenszyklus“ einer Schwachstelle von ihrer Entdeckung bis zur Behebung.

Auftreten von Schwachstellen

Aufgrund der großen Komplexität heutiger Software sind Fehler bei der Entwicklung nur schwer zu vermeiden. Die meisten dieser Fehler sind nicht unmittelbar sicherheitskritisch, oder Schutzmechanismen im Betriebssystem oder in der Software selbst verhindern eine schadhafte Ausnutzung. Moderne Entwicklungsprozesse wie etwa der *Security Development Lifecycle (SDL)* von Microsoft unterstützen zwar die Entwicklung sicherer Software, dennoch treten Schwachstellen nach wie vor häufig auf.

Viele Schwachstellen werden nicht öffentlich bekannt, da ein Hersteller sie im Idealfall selbst entdeckt und behebt, bevor ein Dritter sie finden und insbesondere ein Angreifer sie ausnutzen kann.

Wird eine sicherheitskritische Schwachstelle jedoch nicht durch den Hersteller, sondern durch einen Dritten gefunden, gibt es unterschiedliche Möglichkeiten, wie ihr Lebenszyklus und die daraus resultierende Gefährdung für den Nutzer verlaufen können. Wichtig sind dabei Rolle und Selbstverständnis des Entdeckers. Neben Personen, die sich beruflich mit IT-Sicherheit beschäftigen, kann beispielsweise auch akademische Forschung zur Entdeckung von Schwachstellen beitragen. Es kann sich um gezielte Suche nach Schwachstellen handeln, aber auch Zufallsfunde sind möglich.

Der Lebenszyklus hängt daher stark von Verhalten und Motivation des Entdeckers sowie von der Reaktion des Herstellers ab:

- Ist dem Entdecker daran gelegen, die IT-Sicherheit zu verbessern, oder möchte er die Schwachstelle für eigene, möglicherweise kriminelle Zwecke nutzen?
- Wie viele Informationen über die Schwachstelle werden öffentlich bekannt?
- Schätzt der Hersteller die entstehende Gefährdung richtig ein und kann er schnell genug Abhilfe schaffen?

Um die Diskussion über Schwachstellen zwischen Entdeckern, Herstellern und weiteren Beteiligten zu systematisieren, wurde zur einheitlichen Benennung von öffentlich bekannten Schwachstellen und zur Sammlung der darüber verfügbaren Informationen mit den *Common Vulnerabilities and Exposures (CVE)* ein herstellerübergreifender Industriestandard geschaffen. Mit diesem Standard wird sichergestellt, dass alle Beteiligten während des gesamten Lebenszyklus tatsächlich jeweils dieselbe Schwachstelle meinen. Zudem werden statistische Auswertungen ermöglicht.

Schematischer Lebenszyklus

Grundsätzlich basiert der Lebenszyklus einer durch Dritte entdeckten Schwachstelle auf dem folgenden Schema:

1. Die Schwachstelle wird durch einen Dritten entdeckt und untersucht.
2. Der Hersteller erlangt auf einem der folgenden Wege Kenntnis von der Schwachstelle:
   - Der Entdecker veröffentlicht sämtliche Informationen über die Schwachstelle.
     → *Full Disclosure*
   - Der Entdecker informiert den Hersteller direkt und verzichtet zunächst auf eine detaillierte Veröffentlichung.
     → *Coordinated Disclosure*
   - Die Schwachstelle wird für Angriffe ausgenutzt und diese werden entdeckt.
     → *Zero-Day-Exploit*
   - Der Hersteller wird indirekt über die Schwachstelle informiert.
     → *Schwachstellen-Broker*
3. Der Hersteller beginnt mit der Entwicklung eines *Patches* (von engl. *Flicken*), einer Nachbesserung der Software, mit der die Schwachstelle behoben wird.
4. Der Hersteller veröffentlicht eine Schwachstellenwarnung, ein sogenanntes *Advisory*. Dieses enthält üblicherweise allgemeine Informationen zur Schwachstelle, eine Bewertung der entstehenden Gefährdung sowie mögliche vorläufige Gegenmaßnahmen (sogenannte *Workarounds* oder *Mitigations*). Ein Advisory wird vor allem dann schon vor Verfügbarkeit des Patches veröffentlicht, wenn auch die Öffentlichkeit bereits Kenntnis von der Schwachstelle hat und die Gefährdung hoch ist. Häufig erscheinen Advisory und Patch jedoch zeitgleich.
5. Der Hersteller stellt zusammen mit einer entsprechenden Beschreibung (*Bulletin*) einen Patch zur Behebung der Schwachstelle bereit. Durch Analyse des Patches kann ein Angreifer unter Umständen so viele Details über die Schwachstelle herausfinden, dass er sie ausnutzen kann. Daher steigt mit der Veröffentlichung des Patches die Gefährdung für ungepatchte Systeme an.
6. Der Benutzer der betroffenen Software installiert den Patch, schließt dadurch die Schwachstelle und ist erst dann vor ihrer Ausnutzung geschützt. Dies unterstreicht die enorme Bedeutung eines effektiven Patchmanagements.

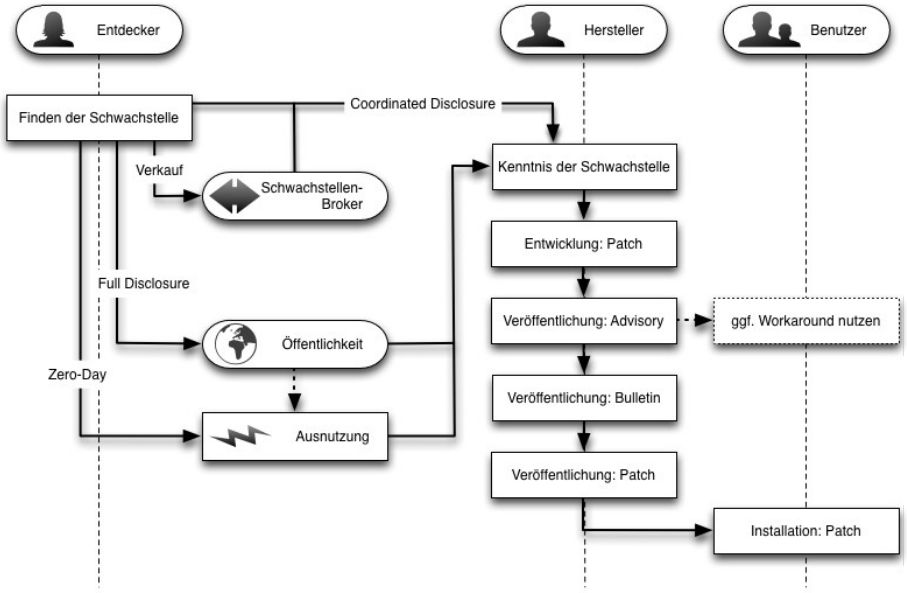

Abbildung 1: Lebenszyklus einer Schwachstelle

Abweichungen von diesem Schema sind möglich, der Ablauf kann sich dynamisch ändern. So kann ein Hersteller beispielsweise eine Schwachstelle als unkritisch einschätzen und auf die Entwicklung eines Patches zunächst verzichten. Wird zu einem späteren Zeitpunkt doch eine Ausnutzungsmöglichkeit bekannt, so kann der Hersteller dadurch zu einer entsprechenden schnellen Reaktion gezwungen sein.

Bekanntwerden von Schwachstellen

Wie im schematischen Lebenszyklus beschrieben hat der Entdecker einer Schwachstelle unterschiedliche Möglichkeiten, mit seiner Entdeckung umzugehen. Dies hat unmittelbare Auswirkungen auf den Hersteller und die Gefährdung der Benutzer des betroffenen Software-Systems. Welche der beschriebenen Möglichkeiten mit welchen Vorteilen und Risiken verbunden ist, hängt stark vom jeweiligen Einzelfall ab.

Full Disclosure

Bei einer *Full Disclosure* stellt der Entdecker einer Schwachstelle alle ihm darüber vorliegenden Erkenntnisse vollständig der Öffentlichkeit zur Verfügung, etwa auf einer entsprechenden Mailingliste. Dies schließt üblicherweise die technischen Details der Schwachstelle sowie Maßnahmen zur Entdeckung und Ausnutzung (sogenannte *Exploits*) ein.

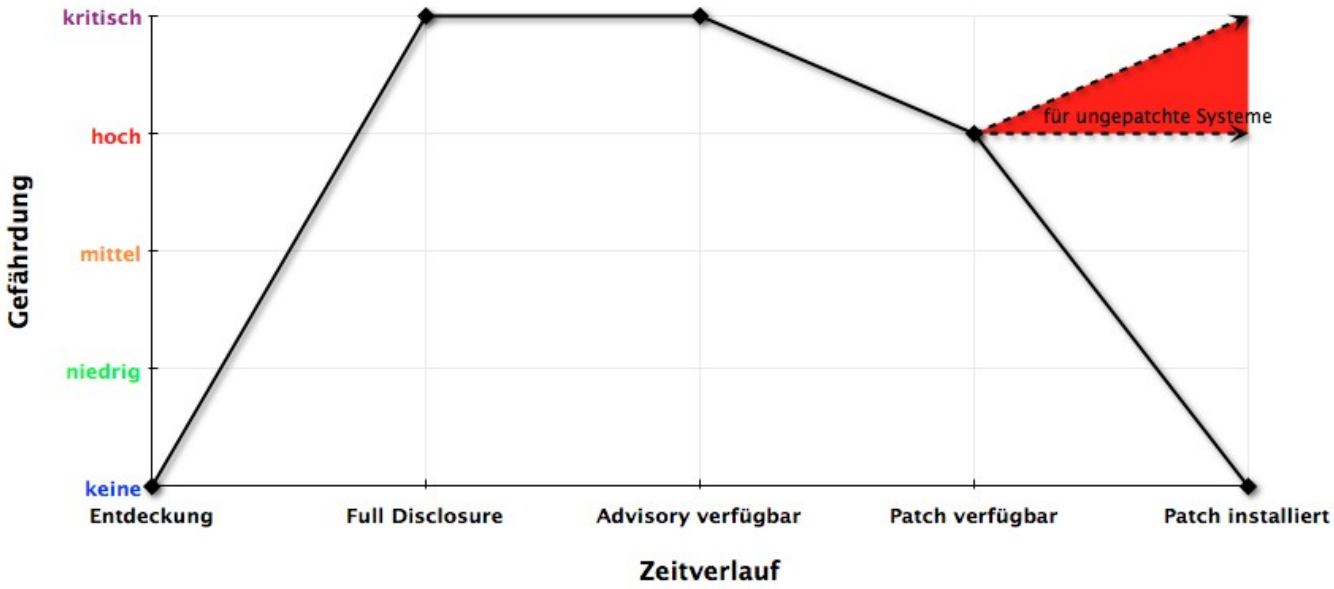

Abbildung 2: Typischer Verlauf der Gefährdung bei Full Disclosure

Das Konzept der Full Disclosure wird kontrovers diskutiert. Verfechter sehen darin einen Weg zur Erhöhung der Sicherheit. Durch die Veröffentlichung ist der betroffene Hersteller gezwungen, möglichst schnell einen Patch bereitzustellen, um Schäden abzuwenden. Dies verkürzt den Gefährdungszeitraum. Außerdem können Hersteller von Schutzprogrammen die veröffentlichten Informationen nutzen, um vorläufige Gegenmaßnahmen zu konzipieren. Kritiker der Full Disclosure führen an, dass eine umfassende Veröffentlichung aller Details die Ausnutzung der Schwachstelle zu bösartigen Zwecken unnötig erleichtert. Entwickler von Schadsoftware bekommen möglicherweise eine einfache Vorlage zur Durchführung von Angriffen auf verwundbare Systeme.

Coordinated Disclosure

Um die offensichtlichen Risiken einer Full Disclosure zu vermeiden, hat sich industrieweit das Konzept der *Coordinated Disclosure* etabliert. Dieses wird häufig auch als *Responsible Disclosure* oder *Limited Disclosure* bezeichnet.

Eine Coordinated Disclosure setzt allgemein eine enge Zusammenarbeit zwischen dem Entdecker der

Schwachstelle und dem Hersteller des betroffenen Produkts voraus. Der Entdecker informiert den Hersteller über seinen Fund und gibt zunächst keine oder nur wenige Informationen an die Öffentlichkeit. Meistens wird nur auf die Existenz und gegebenenfalls auf die Art einer Schwachstelle in einem Produkt hingewiesen. Alle weiteren Details über die Schwachstelle bleiben zunächst einem kleinen Kreis von Personen vorbehalten, zu dem neben Entdecker und Hersteller auch Dritte gehören können, wie etwa Sicherheitsdienstleister und Hersteller von Schutzprogrammen. Stellt der betroffene Hersteller nach Ablauf einer bestimmten Zeitspanne, die im Ermessen des Entdeckers liegt, keinen Patch für die Schwachstelle zur Verfügung, so werden meist doch alle Details an die Öffentlichkeit gebracht (→ Full Disclosure).

Eine Coordinated Disclosure ermöglicht die Diskussion von Schwachstellen, ohne dass Details zu ihrer Ausnutzung in falsche Hände geraten und eine unmittelbare Gefährdung bewirken. Jedoch verleitet dies Hersteller manchmal dazu, Risiken zu unterschätzen, Schwachstellen zu ignorieren oder die Entwicklung von notwendigen Patches hinauszuzögern.

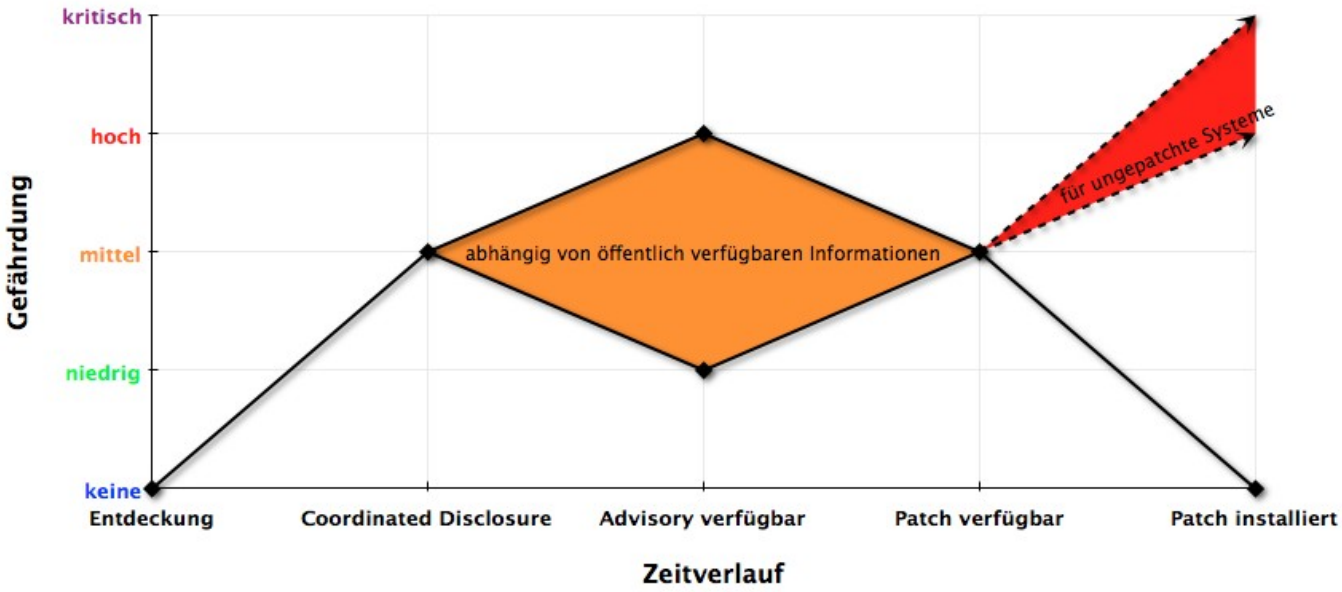

Abbildung 3: Typischer Verlauf der Gefährdung bei Coordinated Disclosure

Zero-Day-Exploit

Die Ausnutzung einer Schwachstelle, die nur dem Entdecker bekannt ist, charakterisiert man mit dem Begriff *Zero-Day-Exploit*. Die Öffentlichkeit und insbesondere der Hersteller des betroffenen Produkts erlangen in der Regel erst dann Kenntnis von der Schwachstelle, wenn Angriffe entdeckt werden, die auf dieser Schwachstelle basieren. Der Begriff *Zero-Day* leitet sich also davon ab, dass ein entsprechender Exploit bereits vor dem ersten Tag der Kenntnis der Schwachstelle durch den Hersteller existierte – also an einem fiktiven „Tag Null“. Der Hersteller hat somit keine Zeit, die Nutzer vor den ersten Angriffen zu schützen.

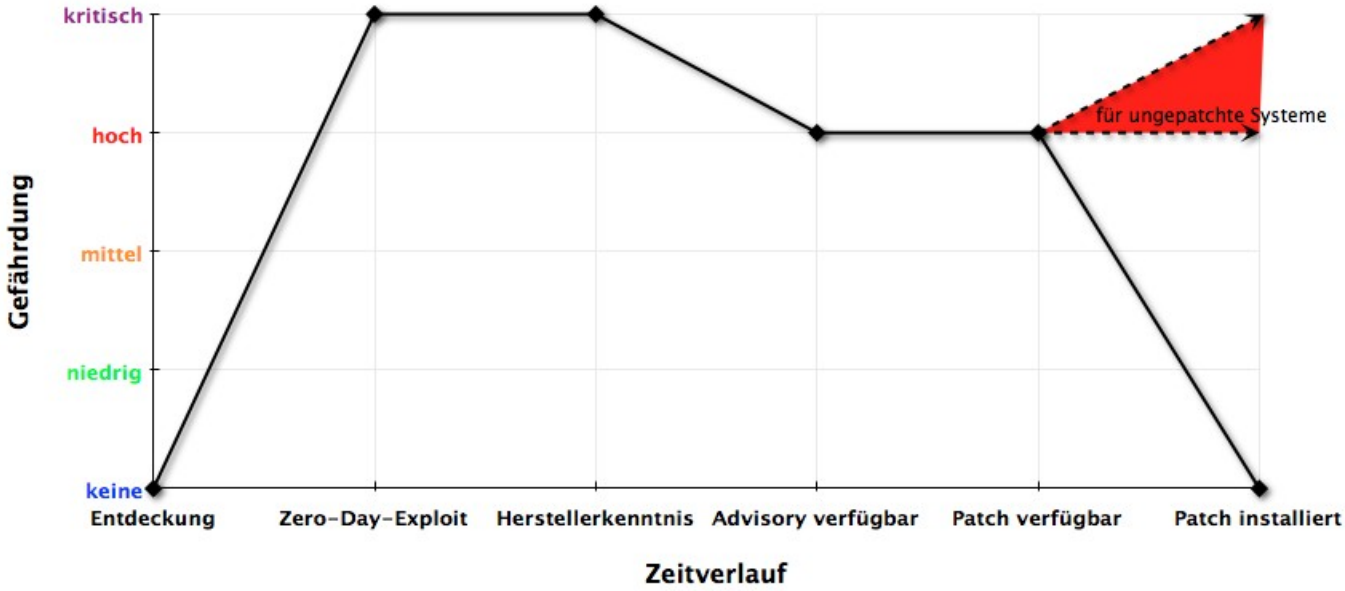

Abbildung 4: Typischer Verlauf der Gefährdung bei einem Zero-Day-Exploit

Angriffe mit einem Zero-Day-Exploit sind effizient, da sie eine Schwachstelle schnell und großflächig ausnutzen können, bevor der Hersteller ein Advisory oder einen Patch bereitstellen kann. Sie stellen daher die größte von einer Schwachstelle ausgehende Gefahr dar.

Bug Bounties und Schwachstellen-Broker

Im Zusammenhang mit dem Suchen und Finden von Schwachstellen haben sich mittlerweile verschiedene Geschäftsmodelle entwickelt. Einige Hersteller, wie etwa Google oder Mozilla, zahlen Entdeckern einen bestimmten Geldbetrag, wenn diese sicherheitskritische Schwachstellen im Rahmen einer Coordinated Disclosure melden. Diese *Bug Bounties*, also „Kopfgelder auf Schwachstellen", können einen deutlichen Anreiz für die Suche nach und die Meldung von Schwachstellen darstellen. Andere Hersteller, wie etwa Adobe und Microsoft, lehnen hingegen eine Bezahlung für die Meldung einzelner Schwachstellen ab.

Auch per Zwischenhandel funktioniert dieses Geschäft: Schwachstellen-Broker wie *TippingPoint (Zero-Day Initiative)* oder *iDefense (Vulnerability Contributor Program)* bezahlen ebenfalls für an sie gemeldete Schwachstellen. Anschließend arbeiten sie üblicherweise mit den betroffenen Herstellern im Rahmen einer Coordinated Disclosure zusammen. Gleichzeitig nutzen sie die erworbenen Informationen, um eigene Dienstleistungen und Produkte zum Schutz vor diesen Schwachstellen anzubieten. Andere Unternehmen, wie beispielsweise *VUPEN,* handeln wiederum auch mit Schwachstellen, die sie unter anderem Geheimdiensten und Ermittlungsbehörden zur Verfügung stellen.

Zusätzlich existieren inoffizielle und zum Teil auch kriminelle Märkte, auf denen insbesondere Zero-Day-Exploits für effiziente Angriffe gehandelt werden.

No Disclosure

No Disclosure bezeichnet einen Spezialfall, der vor allem im Umfeld der Schwachstellen-Broker zu finden ist. Dabei wird der Hersteller vom Entdecker der Schwachstelle nicht informiert, wohl aber die eigenen Kunden, beispielsweise um sie vor Angriffen zu schützen oder um ihnen Zero-Day-Exploits zugänglich zu machen.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an cs-info@bsi.bund.de gesendet werden.