UNIVERSITÄT SIEGEN

Entwicklung eines Online-Formulars zur Meldung von IT-Sicherheitsvorfällen

Dokumentation zur HCI-Master-Projektarbeit

22. März 2016

Sebastian Römer und Sebastian Hörstmann

1. Einführung und Motivation

Diese Projektarbeit beschäftigt sich mit Meldeverfahren von IT-Sicherheitsvorfällen. Hierzu wird ein Meldeformular entwickelt, welches den Austausch über IT-Sicherheitsvorfälle zwischen Organisationen fördern soll. Über eine Plattform zur Meldung von IT-Sicherheitsvorfällen sollen Organisationen schnell auf die Existenz der beschriebenen Sicherheitslücke aufmerksam werden. So können zeitnah Maßnahmen getroffen werden um das eigene System auf Sicherheitslücken zu überprüfen oder präventiv dagegen vorzugehen. Im Ursprung entwickelte sich die Idee ein Meldeformular für IT-Sicherheitsvorfälle zu gestalten durch das am 25. Juli 2015 verabschiedete IT-Sicherheitsgesetz. Hier wird vorgeschrieben, dass Unternehmen, die Betreiber "kritischer Infrastrukturen" sind, Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) melden müssen. Hintergrund dieser Meldepflicht ist unter anderem, dass Angriffe auf Informationstechnologie besser abgewehrt werden können, wenn ein Austausch darüber besteht, welcher Angriff, welche Sicherheitslücke ausnutzt. Es kann so verhindert werden, dass ein Angreifer den gleichen Angriffsvektor nutzt, um Systeme unterschiedlicher Organisationen zu infiltrieren. Die Meldung von IT-Sicherheitsvorfällen dient dabei als "Frühwarnsystem" für andere Organisationen, welche möglicherweise nach dem gleichen Muster angegriffen werden könnten. Dieser Grundsatz soll auf das in dieser Projektarbeit entwickelte Konzept eines Meldeverfahrens übertragen werden. Es wird eine Plattform errichtet, die Awareness über vorgefallene Angriffe auf Informationstechnologie schafft. Dabei steht der Prozess der Erhebung von Daten über IT-Sicherheitsvorfälle und die Darstellung der dabei erhobenen Informationen im Mittelpunkt dieser Projektarbeit. Die Datenerhebung erfolgt über ein Online-Formular, welches Teil der Plattform ist, auf welcher gemeldete Vorfälle wiederum für andere Nutzer zugänglich gemacht werden.

2. State-of-the-Art von Meldeverfahren

Dieser Abschnitt gibt einen groben Umriss über den derzeitigen State-of-the-Art von Meldeverfahren von IT-Sicherheitsvorfällen. Als Grundlage der inhaltlichen Ausarbeitung des Fragenkatalogs für das zu entwickelnde Meldeformular wird eine Recherche über den derzeitigen Stand von Meldeverfahren durchgeführt. Es werden an dieser Stelle die für die Gestaltung des Meldeformulars relevanten Ergebnisse dieser Recherche kurz ausgeführt. Die Recherche umfasst wissenschaftliche Arbeiten sowie Best-Practices von aktuellen Meldeverfahren von IT-Sicherheitsvorfällen.

Wissenschaftliche Arbeiten befassen sich in diesem Bezug größtenteils mit Taxonomien und Klassifizierungen von Angriffen auf Informationstechnologie. Typischerweise werden dabei Modelle vorgestellt, wonach ein Angriff nach verschieden Aspekten klassifiziert wird. Für diese Projektarbeit wird die Taxonomie von Simmons et al.[1] zugrunde gelegt. Diese geht als Ergebnis einer vergleichenden Studie von Taxonomien verschiedener Autoren hervor. Abbildung 1 zeigt diejenigen Kategorien nach denen der Angriff nach Simmons et al. klassifiziert wird.

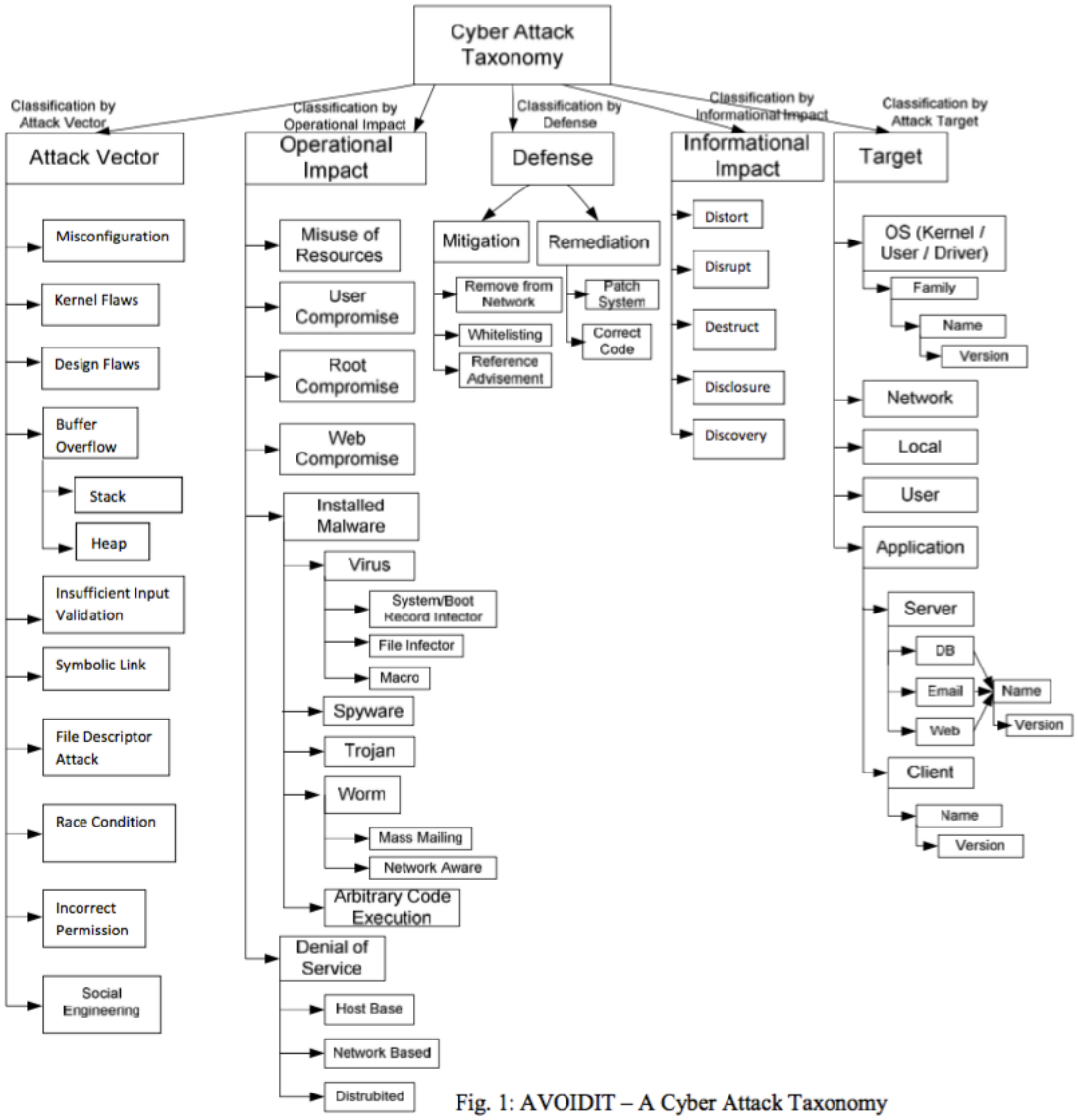


Fig. 1: AVOIDIT – A Cyber Attack Taxonomy

[1] Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., & Wu, Q. (2009). AVOIDIT: A cyber attack taxonomy.

Jede dieser Kategorien hat weitere Unterkategorien, welche die einzelnen Kategorien weiter ausführen. Beispielsweise gehören zur Kategorie *Attack Vector* die Unterkategorien *Misconfiguration*, *Kernel Flaws*, *Design Flaws*, etc.. Auf ähnliche Weise soll der Angriff für das zu entwickelnde Meldeformular beschrieben werden: durch Aufteilung in verschiedene **Kategorien**, welche durch **Unterkategorien** weiter ausgeführt werden.

Diese Vorgehensweise findet man bei vielen in der Praxis eingesetzten Meldeverfahren wieder. Bei der Recherche werden verschiedene Meldeverfahren hinsichtlich ihrer Relevanz für diese Projektarbeit untersucht. Besonderen Einfluss haben dabei die Online-Meldeformulare des amerikanischen *US-CERT*[2] *(United States Computer Emergency Readiness Team)* und der deutschen *Allianz für Cyber-Sicherheit*[3] für das Ergebnis dieser Projektarbeit. Das US-CERT ist Teil des *Department of Homeland Security* und befasst sich mit Sicherheitsrisiken in der IT, sowie mit der Aufrechterhaltung von IT-Sicherheitsstandards und der Kommunikation von IT-sicherheitsrelevanten Themen. Unter anderem veröffentlicht das US-CERT die "*Federal Incident Notification Guidelines*"[4], welche als Grundlage zur Entwicklung des in dieser Arbeit vorgestellten Meldeformulars herangezogen werden. In Deutschland befasst sich die Allianz für Cyber-Sicherheit als Initiative des BSI mit den oben genannten Themen. Dabei steht hier genau wie bei dieser Projektarbeit der Informations- und Erfahrungsaustausch im Vordergrund. Auch das von dieser Institution entwickelte Meldeformular fließt inhaltlich in das im nächsten Abschnitt vorgestellte Konzept ein.

3. Inhaltliches Konzept

Auf Grundlage des oben beschriebenen State-of-the-Art von Meldeverfahren wird das Konzept einer Plattform entwickelt, welche den Austausch von IT-Sicherheitsvorfällen fördert und somit Awareness über aktuelle Ereignisse der Cyber-Kriminalität schafft. Strukturell besteht die Plattform aus den Elementen des **Informationsgewinns** und der **Informationsdarstellung**. Der Gewinn von Informationen über einen vorgefallenen Angriff auf IT bei einer Organisation, erfolgt über ein Online-Meldeformular. Hierzu wird ein **Fragenkatalog** entwickelt (s. Abschnitt 3.1.), welcher ausgefüllt wird, um einen Angriff genauer zu beschreiben. Nach Absenden dieses Meldeformulars werden **Angriffsdetails** (s. Abschnitt 3.2.) zur Beschreibung des gemeldeten Angriffs generiert, welche für alle Teilnehmer der Plattform in einer **Timeline** von aktuellen Angriffen verfügbar ist.

Als zusätzliches Feature der Plattform wird eine **Meldeempfehlung** an den Meldenden ausgesprochen. Durch die im Meldeformular erhobenen Daten kann grob eingeschätzt werden, ob der IT-Sicherheitsvorfall der Meldepflicht nach dem IT-Sicherheitsgesetz unterliegt oder nicht. Ist dies der Fall, erhält der Meldende eine kurze Mitteilung, dass er den Vorfall gegebenenfalls auch dem BSI melden sollte.

---

[2] https://www.us-cert.gov/forms/report

[3] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/Online_Meldung/onlinemeldung.html;jsessionid=675C28F53815F725B8F0964B449EFC97.2_cid351

[4] https://www.us-cert.gov/incident-notification-guidelines

3.1. Der Fragenkatalog als Quelle des Informationsgewinns

Der oben beschriebene State-of-the-art ist die Grundlage des entwickelten Fragenkatalogs. Zusätzlich wurden Vorschriften aus dem kürzlich erschienenen IT-Sicherheitsgesetz berücksichtigt, um die Meldeempfehlung zu realisieren. Bei der Gestaltung des Fragenkatalog wird darauf geachtet, dass dieser weitestgehend automatisiert ausgefüllt werden kann. Das heißt, dass möglichst viele Antwortmöglichkeiten bereits durch das System vorgeschlagen werden sodass, der Nutzer nur die passenden auswählen muss. Somit sind gemeldete IT-Sicherheitsvorfälle besser vergleichbar. Dennoch muss trotz der Automatisierung genügend Freiraum für eigene Formulierungen des Nutzers gelassen werden, da sonst eventuell wichtige Informationen verloren gehen würden. Im Folgenden wird der Aufbau und Inhalt des Fragenkatalogs zur Meldung von IT-Sicherheitsvorfällen erläutert. Dieser unterteilt sich in drei Bereiche: Kontakt-, Vorfalls-, und Angriffsinformationen.

KONTAKTINFORMATIONEN

Kontaktinformationen werden angegeben, damit der Autor für Rückfragen erreichbar ist. Hierbei lässt sich über Pflicht und Optionalität der Angaben diskutieren. Eine weitere Möglichkeit würde darin bestehen, das Formular gänzlich anonym ausfüllen zu lassen. In diesem Falle müsste aber trotzdem eine Möglichkeit gegeben sein, den Autor bei Rückfragen zu kontaktieren. Nach dem IT-Sicherheitsgesetz soll es möglich sein, einen Vorfall bis zu einem gewissen Maß pseudonymisiert zu melden (§8b, Absatz 4). Demnach müsse man die Identität seiner Organisation und seine eigene nicht angeben, solange man auf andere Weise (anonym) erreichbar bleibt. Da sich diese Projektarbeit primär mit der Gestaltung des Online-Formulars selbst beschäftigt, wird der Problematik der Anonymität nicht weiter nachgegangen. Folgende Angaben macht der Autor bezüglich seiner Organisation und seinen Kontaktinformationen:

Vor- und Nachname: Namen werden nicht veröffentlicht, sondern dienen nur zur Identifikation.

Organisation: Nach dem IT-Sicherheitsgesetz muss in besonderen Fällen muss die Organisation veröffentlicht werden.
Branche der Organisation: Die Angabe der Branche gewährleistet Vergleichbarkeit zur Branche des Meldenden.

Rolle des Autors in der Organisation: Die Rolle des Autors in der Organisation impliziert (in den meisten Fällen) Informationen über seine Expertise im Bereich der IT-Sicherheit.

E-Mail-Adresse: Der Autor soll per E-Mail für Rückfragen erreichbar sein.

Telefonnummer: Es könnten besonders dringende Fälle eintreten, bei denen der Autor auch per Telefon erreichbar sein soll.

Ist die betroffene Organisation eine "kritische Infrastruktur"?: Betreiber von kritischen Infrastrukturen unterliegen in bestimmten Fällen der Meldepflicht von IT-Sicherheitsvorfällen gegenüber dem BSI.

VORFALLSINFORMATIONEN

Zur Beschreibung des IT-Sicherheitsvorfalls wird zwischen Vorfalls- und Angriffsinformationen unterschieden. Vorfallsinformationen umfassen allgemeine Angaben zum zeitlichen Rahmen und zu den Auswirkungen des Vorfalls. Im Folgenden werden diese Angaben erläutert.

Zeitlicher Rahmen des Vorfalls

Folgende Angaben werden bezüglich des zeitlichen Rahmens gemacht:

Entdeckungszeitpunkt: Wann ist man auf den Vorfall aufmerksam geworden?

Startzeitpunkt: Welcher ist der frühste Zeitpunkt, auf welchen sich der Vorfall zurückverfolgen lässt?

Dauert der Vorfall noch an?: Sind zum aktuellen Zeitpunkt noch Aktivitäten des Vorfalls festzustellen?

Endzeitpunkt: Wann wurden die letzten Aktivitäten des Vorfalls festgestellt?

Hat der Vorfall Auswirkungen auf die Vertraulichkeit, Integrität oder Verfügbarkeit Ihrer Systeme?

Der Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit (CIA-Prinzip) von Systemen gilt in der IT-Sicherheit als die grundlegende Bedrohung. Die hier gestellte Frage wird zunächst nur mit “Ja” oder “Nein” beantwortet, da sich die kommenden Fragen im Falle keiner Auswirkungen (wenn mit “Nein” geantwortet wird) erübrigen würden. Anschließend wird nach der Ausprägung der Auswirkungen des Vorfalls gefragt.

Wie hoch sind die Funktionalen Auswirkungen des Vorfalls?

Funktionale Auswirkungen umfassen sämtliche Störungen des Arbeitsbetriebes. Die Frage nach der Höhe der funktionalen Auswirkungen gibt Rückschlüsse auf die Schwere des IT-Sicherheitsvorfalls. Diese ist notwendig um eine Meldeempfehlung für das BSI auszusprechen. Nach dem IT-Sicherheitsgesetzt müssen “erhebliche” Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von Systemen, Prozessen und Komponenten gemeldet werden (§8b, Absatz 4). Nach den *US-CERT Federal Incident Notification Guidelines* werden folgende Ausprägungen unterschieden, welche für diesen Fragenkatalog übernommen werden:

Hoch: Die Funktionsweise von kritischen Diensten wurde für alle Nutzer eingeschränkt

Mittel: Die Funktionsweise von kritischen Diensten wurde für einige Nutzer eingeschränkt

Niedrig: Alle Dienste sind für alle Nutzer uneingeschränkt nutzbar, jedoch bestehen Einschränkungen in der Performanz der Dienste.

Keine: Es bestehen keinerlei Einschränkungen bezüglich der Nutzung aller Dienste.

Inwiefern bestand unauthorisierter Zugriff auf vertrauliche Informationen?

Im Gegensatz zu funktionalen Auswirkung hat der unauthorisierte Zugriff auf Informationen keine direkte Störung des allgemeinen Arbeitsbetriebes zur Folge. Die Gefährdung entsteht dadurch, dass der Angreifer vertrauliche Informationen einsehen, kopieren, löschen oder ändern kann. Die Modifizierung von Informationen kann wiederum funktionale Auswirkungen nach sich ziehen. Nach den *US-CERT Federal Incident Notification Guidelines* werden folgende Ausprägungen unterschieden, welche für diesen Fragenkatalog übernommen werden:

Geheim: Die Vertraulichkeit von streng geheimen Informationen wurde gefährdet.

Geschützt: Die Vertraulichkeit von geschützten firmenkritischen Daten wurde gefährdet.

Privat: Die Vertraulichkeit von persönlichen Informationen wurde gefährdet.

Integrität: Die notwendige Integrität von Informationen wurde gefährdet.

Keine: Es bestand keinerlei Gefährdung vertraulicher Informationen.

ANGRIFFSINFORMATIONEN

Im Abschnitt Angriffsinformationen wird der Angriff im Detail beschrieben. Im Kern umfasst der Fragenkatalog an dieser Stelle Angaben über den **Angriffsvektor**, das **Angriffsziel** (das betroffene System), die **Angriffsart**, sowie die vermutete **Intention** des Angriffs. Zu jeder Angabe hat der Autor die Möglichkeit weitere wichtige Informationen zu dieser Angabe als Freitext mitzuteilen, die andernfalls verloren gehen würden.

Wie wurde der Angriff erkannt?

Zunächst soll der Autor beschreiben, wie er auf den Angriff aufmerksam geworden ist. Ziel hiervon ist, dass der Angriff von anderen auf die gleiche Weise entdeckt werden kann. Folgende Antwortmöglichkeiten werden gegeben, um zu anzugeben, welche Person oder welches System den Angriff erkannt hat:

Administrator

Benutzer

Log-Review eines Analysten

Intrusion Detection System

Anti-Viren-Software

Andere

Unbekannt

Nachdem ausgewählt wurde, von wem der Angriff erkannt wurde, hat der Autor im nächsten Schritt die Möglichkeit genauer zu beschreiben, wie der Angriff erkannt wurde. Dabei sollte er

diesen Prozess möglichst detailliert und Schritt-für-Schritt beschreiben, damit ihn andere nachvollziehen und somit den Angriff bei sich selbst auf die gleiche Weise erkennen können.

Welches System wurde angegriffen?

Der Autor gibt an, welche Software oder Hardwarekomponente bei diesem Angriff betroffen war. Dadurch sollen andere Nutzer, die das gleiche System verwenden, vor möglichen Sicherheitslücken gewarnt werden. Außerdem ist diese Information notwendig, um dem Autor im weiteren Verlauf des Formulars passende CVE-Einträge vorzuschlagen, welche die angegriffene Schwachstelle weiter definieren.

Wodurch wurde der Angriff ermöglicht?

An dieser Stelle wird der Angriffsvektor definiert. Es werden hierzu verschiedene Auswahlmöglichkeiten dazu gegeben, wodurch der Angriff ermöglicht wurde. Hierbei handelt es sich um typische Angriffsvektoren, die statistisch die häufigsten bei IT Angriffen sind. Sollte keiner der zur Auswahl stehenden Vektoren passend sein, hat der Autor die Möglichkeit einen eigenen Angriffsvektor zu nennen. Es gibt folgende Antwortmöglichkeiten, welche sich teilweise kategorisch zusammenfassen lassen:

Miskonfiguration: Der Angriff erfolgte über eine Schwachstelle, die auf einen Konfigurationsfehler zurückzuführen ist. Dabei können folgende Arten von Konfigurationsfehlern spezifiziert werden:

- Falsche Berechtigung
- veraltete Systemversion
- ungenutzte Features aktiviert
- Standardeinstellungen beibehalten

USB-Geräte: Schädliche Software wurde über ein USB Medium übertragen.

E-Mail: Schädliche Software wurde über E-Mail übertragen.

Unzureichende Eingabevalidierung: Input-Felder werden nicht ausreichend validiert, sodass schädlicher Code infiltriert werden konnte. Folgende Arten "unzureichender Eingabevalidierung" können spezifiziert werden:

- Cross-Site-Scripting
- SQL Injection
- Buffer Overflow
- Cross-Site-Request-Forgery

Botnetz: Ein großer Zusammenschluss von mit Malware infizierten PCs ermöglichte den Angriff.

Identitätsdiebstahl: Der Angriff wurde dadurch ermöglicht, dass sich der Angreifer eine vertrauenswürdige Identität verschafft hat. Dabei können folgende Arten spezifiziert werden:

- Man-In-The-Middle
- Phishing
- Spoofing
- Pharming

Ausnutzen einer Sicherheitslücke eines IT-Produktes: Der Angriff wurde durch einen Design- oder Implementierungsfehler eines IT-Produktes ermöglicht.

Social Engineering: Der Angriff wurde dadurch ermöglicht, dass firmeninterne Personen zu sicherheitskritischen Handlungen gedrängt wurden.

Welche Art des Angriffs wurde ermöglicht?

Die Art des Angriffs bezieht sich auf die eigentliche Ausführung des Angriffs. Im vorigen Abschnitt wurde definiert über welchen Vektor der Angriff stattgefunden hat, während an dieser Stelle definiert wird, welche Art von Angriff über diesen Vektor stattgefunden hat. Bei den folgenden Auswahlmöglichkeiten handelt es sich um die typischsten Arten von Angriffen:

Schadprogramm

- Virus
- Wurm
- Trojanisches Pferd
- Adware, Spyware

Denial-of-Service

Beliebige Codeausführung

Welcher Zweck wurde vermutlich durch den Angriff verfolgt?

Der Zweck des Angriffs definiert die Intention des Angreifers. Mit dem Wissen darüber, welches übergeordnete Ziel bei dem Angriff verfolgt wurde, ist es für andere leichter Maßnahmen zur Vorbeugen zu treffen. Hier werden Antwortmöglichkeiten geben, die aus dem Meldeformular der *Allianz für Cyber-Sicherheit* übernommen werden:

Erpressung

Identitätsdiebstahl

Entwendung vertraulicher Information

Störung der Geschäftstätigkeit

Sabotage / Denial-of-Service

Manipulation von Daten

Nutzung von Systemressourcen (Spam-Relay, Botnetz-Client, C&C-Server, Dropzone-Server)

Defacement: unberechtigtes Ändern einer Webseite durch den Angreifer

Können Sie die ausgenutzte Schwachstelle definieren?

Aufgrund der Angaben, die der Autor weiter oben über das angegriffene System tätigt, lässt sich die CVE Datenbank[5] durchsuchen. An dieser Stelle werden dann CVE Einträge vorgeschlagen, welche die vorliegende Schwachstelle des Systems eventuell beschreiben. Der Autor erhält eine Liste von für das System zutreffenden Vorschlägen, aus der er einen auswählen kann. Sollte die Liste keinen passenden Eintrag enthalten, kann er alternativ selbst einen CVE Eintrag angeben oder gänzlich auf eine Angabe verzichten.

Wie haben Sie auf den Angriff reagiert?

An dieser Stelle soll der Autor Maßnahmen beschreiben, die ergriffen wurden, um das betroffene System wiederherzustellen bzw. die Schwachstelle zu beheben. Dies kann anderen Nutzern helfen selbst gegen den Angriff vorzugehen oder diesen vorzubeugen. Außerdem kann der Autor seine Problematik schildern, wenn er selbst daran scheitert das System wiederherzustellen.

Welche Maßnahmen wurden ergriffen?

Wie groß schätzen Sie den Aufwand das System wiederherzustellen?: Um einheitliche und vergleichbare Aussagen zu dieser Frage tätigen zu könnten, werden hier Auswahlmöglichkeiten gegeben welche sich an den US-CERT Federel Incident Notification Guidelines orientieren:

- **Nicht wiederherstellbar**: Die Wiederherstellung des Systems ist nicht möglich.
- **Externe Hilfe**: Die Zeit zur Wiederherstellung ist nicht vorauszusehen, es wird externe Hilfe benötigt.
- **Ergänzende Ressourcen**: Die Zeit zur Wiederherstellung ist mit ergänzenden Ressourcen vorauszusehen.
- **Vorhandene Ressourcen**: Die Zeit zur Wiederherstellung ist mit vorhandenen Ressourcen vorauszusehen.
- **Nicht anzuwenden**: Der Angriff erfordert keine Wiederherstellung.

Ist das betroffene System bereits wiederhergestellt?

[5] https://cve.mitre.org

3.2. Die Angriffsdetails als Informationsdarstellung

Wenn ein IT-Sicherheitsvorfall gemeldet wird, wird dieser für alle zugänglich in einer Timeline veröffentlicht. Neue Einträge werden in der Timeline an oberster Stelle angezeigt und mit Tags versehen, die helfen sollen auf den ersten Blick einen Eindruck über den dahinter liegenden Vorfall zu bekommen. Für detaillierte Informationen zu einzelnen Vorfällen, werden Einträge aus der Timeline aufgerufen. Die Detailansicht eines IT-Sicherheitsvorfalls ist genau wie das Meldeformular in kategorische Abschnitte eingeteilt. Diese werden im Folgenden erläutert.

Allgemeine Informationen

Zunächst werden allgemeine Informationen dargestellt, wann und von wem der Vorfall gemeldet wurde, sowie der Titel des Vorfalls. Hierbei wird jedoch nicht die Identität des Autors preisgegeben, um eine schlechte Reputation für ihn und seine Organisation zu vermeiden. Stattdessen wird lediglich seine Rolle in der Organisation, die Aufschluss über seine Expertise bringt, und die Branche seiner Organisation, welche Vergleichbarkeit für andere Nutzer der gleichen Branche liefert, dargestellt.

Zeitlicher Rahmen

Angaben über den zeitlichen Rahmen beinhalten den Start- und Endzeitpunkt, sowie den Erkennungszeitpunkt des Vorfalls.

Angriffsbeschreibung

In diesem Abschnitt wird beschrieben, was beim Angriff vorgefallen ist. Es werden die Angaben des Autors über den **Angriffsvektor**, **Art** des Angriffs, **Angriffszweck** und das **betroffene System** dargestellt.

Schwachstelle im System bzw. der Anwendung

Im Bezug auf das betroffene System wird an dieser Stelle der ausgewählte bzw. händisch eingetragene CVE-Eintrag angezeigt, sowie weitere Informationen, welche der Autor bezüglich der Schwachstelle gegeben hat.

Den Angriff erkennen

Der Autor hat beim Ausfüllen des Meldeformulars den Prozess beschrieben, wie er auf den Angriff aufmerksam geworden ist. Dieser wird hier dargestellt, sodass der Leser ihn nachvollziehen kann und gleiche Maßnahmen ergreifen kann, um den Angriff in seinem System zu erkennen.

Lösung

Sollte der Autor bereits selbst einen Lösungsweg zur Wiederherstellung des angegriffenen Systems beschrieben haben, wird dieser hier dargestellt. Außerdem wird der Aufwand zur Systemwiederherstellung angezeigt, sowie die Angabe, ob das System komplett, teilweise oder gar nicht wiederhergestellt werden konnte.

Autor kontaktieren

Wenn es auf Seiten des Lesers Rückfragen geben sollte oder er Hilfestellung bezüglich des geschilderten IT-Sicherheitsvorfall leisten könnte, kann er hier eine E-Mail an die vom Autor hinterlegte E-Mail-Adresse senden.

4. Technisches Konzept

Für die technische Umsetzung des in Abschnitt 3 beschriebenen inhaltlichen Konzepts werden verschiedene Technologien und Frameworks verwendet, welche in Abbildung 2 veranschaulicht werden:

- **AngularJS**[6] zum dynamischen Umgang mit HTML Seiten,
- **Baasbox**[7] zum Speichern und Abrufen von gemeldeten Sicherheitsvorfällen
- **Node.js**[8] als Serverumgebung für die zu entwickelnde API als Schnittstelle zur CVE-Datenbank

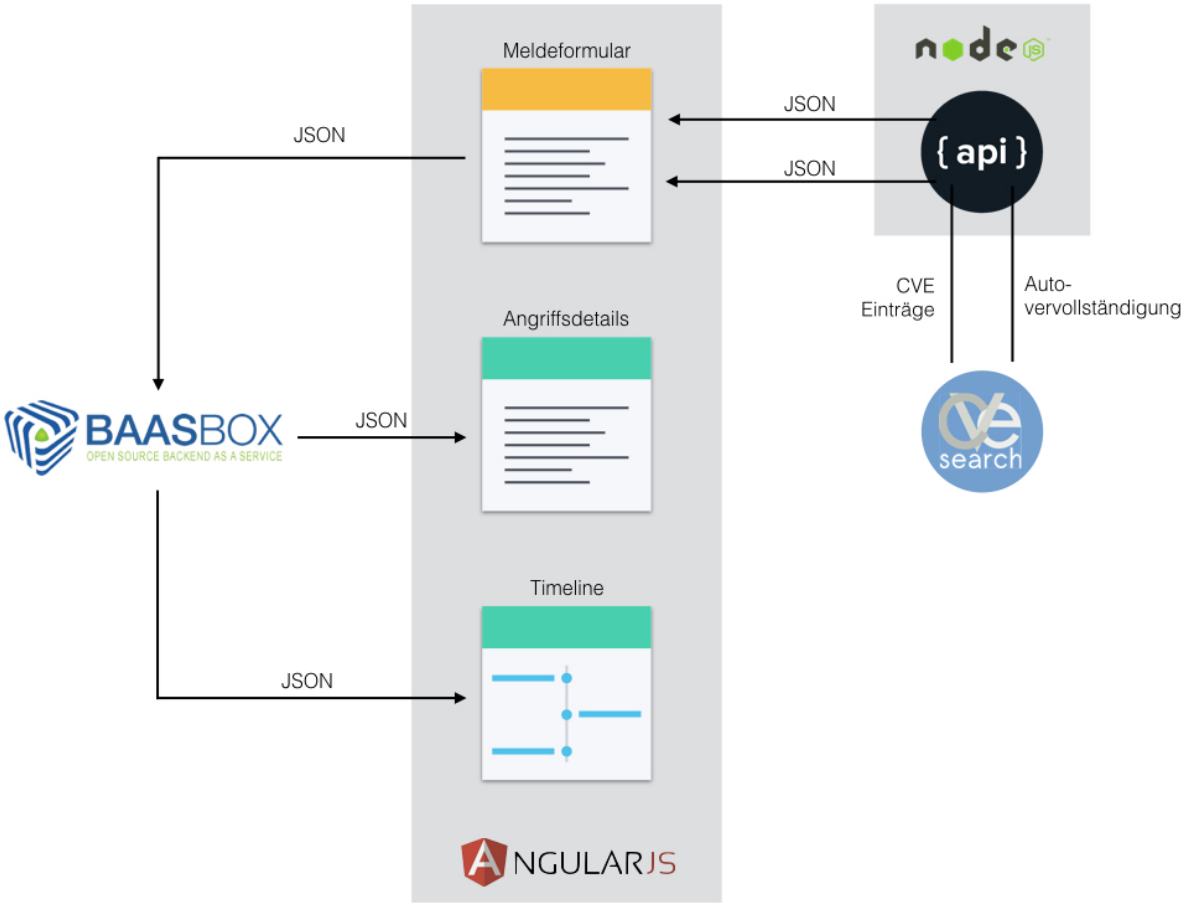


Abbildung 2: Technisches Konzept

[6] https://angularjs.org

[7] http://www.baasbox.com

[8] https://nodejs.org

Die zu entwickelnde Online-Plattform zur Meldung und Darstellung von IT-Sicherheitsvorfällen wird als Website bestehend aus HTML Seiten realisiert. Da die Nutzung des Online-Meldeformulars gewisse Dynamiken erfordert, welche mit reinem HTML nur aufwendig implementiert werden können, wird hierzu das **AngularJS** Framework verwendet. Das Meldeformular passt sich im Laufe des Meldeverfahrens ständig an die Eingaben des Nutzers an. In Abhängigkeit von bestimmten Antworten auf bestimmte Fragen, werden beispielsweise weitere tiefergehende Fragen gestellt. Die Verwendung von AngularJS vereinfacht die Umsetzung dieser Dynamiken des Meldeverfahrens sehr. Des Weiteren wird AngularJS dazu genutzt um Angaben des Nutzers in einer **JSON** Datei immer wieder zu zwischenzuspeichern, während er das Meldeformular ausfüllt. Hierzu wird ein **Model**[9] definiert, welches alle Angaben des Meldeformulars enthält. Die einzelnen Fragen des Formulars werden an zugehörige Attribute des Models gebunden, sodass dieses zu jedem Zeitpunkt den aktuellen Status des bis dahin ausgefüllten Meldeformulars repräsentiert.

Wenn das Meldeformular vollständig ausgefüllt wurde, wird das zwischengespeicherte Model als JSON Datei mithilfe von **Baasbox** dauerhaft abgelegt und verfügbar gemacht. Baasbox stellt das Model der Timeline und den Angriffsdetails als Abbild des gemeldeten IT-Sicherheitsvorfalls zur Verfügung, wo es wiederum durch AngularJS ausgelesen und dargestellt wird.

Im Abschnitt *Angriffsinformationen* des Meldeformulars wird das angegriffene System angegeben. Hier soll der Name der betroffenen Soft- oder Hardware eingetragen werden. Damit hier einheitliche und konsistente Namen angegeben werden, wird eine Autovervollständigung verwendet, welche aus einer Datenbank von Soft- und Hardware Vorschläge macht. Hierzu wird die **CVE-Search API**[10] genutzt. CVE-Search liefert eine Liste von Herstellern und zugehörigen Produkten, welche durch das Tippen von Buchstaben in das Feld der Autovervollständigung gefiltert wird. Durch jeden neu eingegebenen Buchstaben wird die Liste weiter gefiltert, bis der Nutzer einen der vorgeschlagenen Hersteller und Produkte auswählt. Des Weiteren wird die CVE-Search API genutzt, um CVE-Einträge abzufragen. Mithilfe des angegeben Produktes liefert die CVE-Search Datenbank zugehörige CVE-Einträge, welche dem Nutzer angezeigt werden, damit er einen passenden auswählen kann. Als Schnittstelle zwischen dem Online-Formular und der CVE-Search API wird eine eigens entwickelte API gesetzt. Diese wird genutzt, um die von der CVE-Search API gelieferten Ergebnisse passend für das Formular aufzuarbeiten. Die aufgearbeiteten Daten werden schließlich als JSON Datei an das Online-Formular übergeben. Die Client-Server-Architektur, welche Requests und Responses der entwickelten API verwaltet, wird mithilfe von **Node.js** implementiert.

[9] https://docs.angularjs.org/api/ng/directive/ngModel

[10] https://github.com/cve-search/cve-search

5. Implementierung des Online-Formulars als Prototyp

Das erste konzeptuelle Design des Prototypen wurde mit **Sketch**[11] entwickelt. Hierzu wurden Designvorlagen von **Bootflat**[12] als Teil von **Bootstrap**[13] verwendet. Im folgenden werden Screenshots des vollfunktionsfähigen Prototypen als Ergebnis der Implementierung der Website dargestellt. Dabei werden lediglich designtechnische und keine inhaltlichen Aspekte beschrieben. Das inhaltliche Konzept wurde bereits weiter oben in Abschnitt 3 erläutert.

Der Prozess der Meldung eines IT-Sicherheitsvorfalls erfolgt in vier Schritten: Angabe der Kontaktinformationen, Beschreibung des Vorfalls, Beschreibung des Angriffs und Überprüfung der Eingaben. Der Header des Meldeformulars (s. Abbildung 3) zeigt an, an welchem der Schritte man sich derzeit befindet. Außerdem kann er dazu genutzt werden, um zwischen den einzelnen Schritten zu navigieren (durch Klicken auf den jeweiligen Schritt).

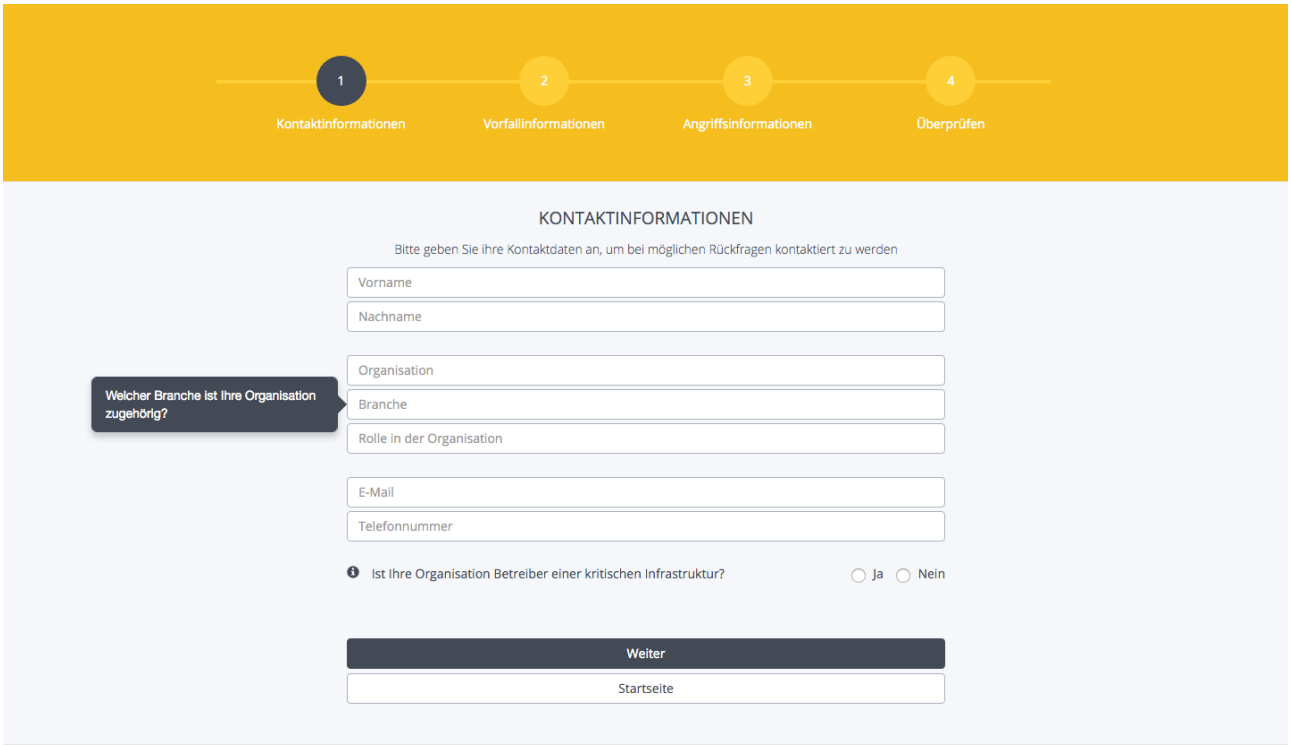


Abbildung 3: Kontaktinformationen

Abbildung 3 zeigt die Implementierung des Formulars zur Angabe der Kontaktinformationen. Eingabefelder werden mit Tooltips versehen, damit diese nicht fehlinterpretiert werden. Tooltips erscheinen, wenn sich der Mauszeiger über dem entsprechenden Feld befindet. Außerdem gibt es einen Info-Button (i), welcher den Begriff der "kritischen Infrastruktur" erläutert. Das Info-Feld wird angezeigt, wenn der Button gedrückt wird und verschwindet wieder, sobald an eine beliebige andere Stelle geklickt wird. Diese Art der Interaktion wird gewählt, da der Inhalt der Info-Felder teilweise komplexer ist. Daher werden diese durch klicken über einen längeren Zeitraum angezeigt und verschwinden nicht wieder wenn der Mauszeiger seine Position verlässt.

[11] https://www.sketchapp.com

[12] http://bootflat.github.io

[13] http://getbootstrap.com

Abbildung 4 zeigt das Formular zur Beschreibung der Vorfallsinformationen. Zur Definition des zeitlichen Rahmens des Vorfalls werden Datums- und Zeitfelder verwendet. Durch Klicken in das Datumsfeld öffnet sich ein Kalender, in dem ein Datum ausgewählt werden kann. Die Uhrzeit kann per Tastatur oder durch "hoch" und "runter" Buttons innerhalb des Zeitfeldes eingetragen werden. Wird die Frage "Dauert der Vorfall noch an?" mit "Ja" beantwortet erscheint eine weitere Datums- und Zeitabfrage zur Angabe des Endzeitpunkts, die andernfalls verborgen bleibt. Ähnliches betrifft die Frage nach den Auswirkungen des Vorfalls. Wird sie mit "Ja" beantwortet, werden tiefergehende Angaben zu den Auswirkungen gemacht. Zu den Fragen "Wie hoch sind die funktionalen Auswirkungen?" und "Inwiefern bestand unautho risiereer Zugriff auf vertrauliche Informationen?" gibt es vordefinierte Antworten, welche per Dropdown-Liste ausgewählt werden. Auch hier werden wieder Info-Buttons verwendet, um weitere Erläuterungen zu einzelnen Fragen zu liefern.

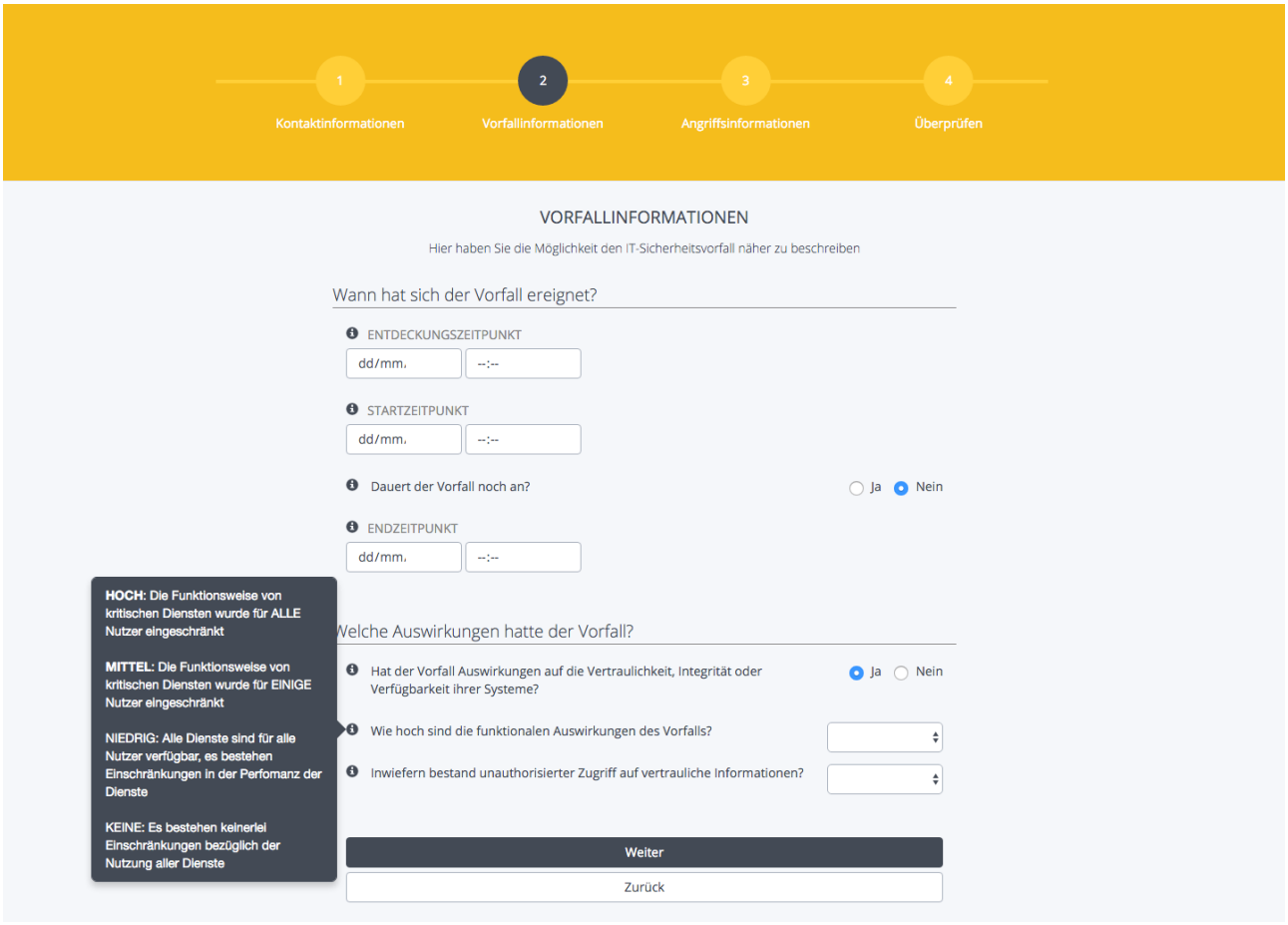
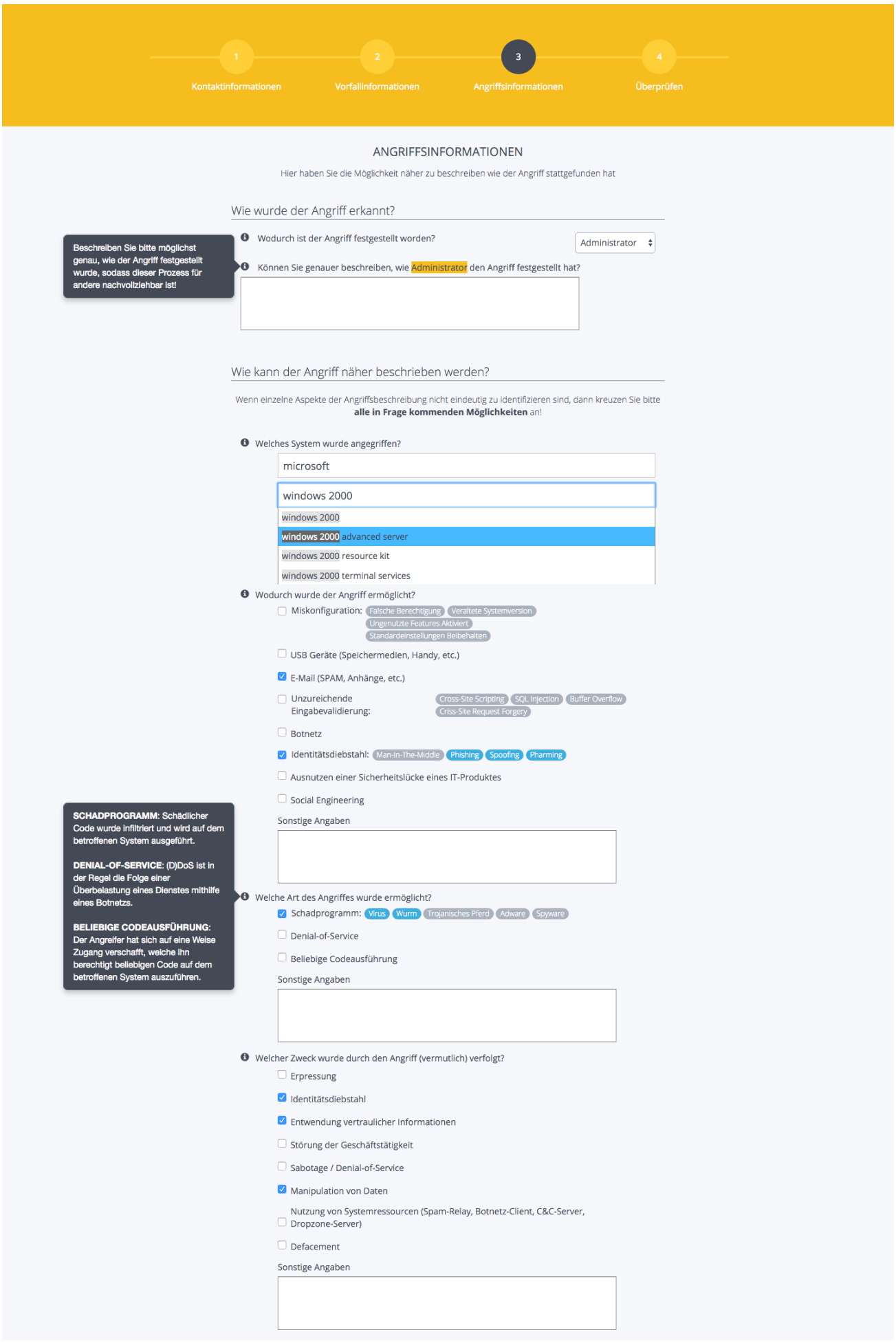


Abbildung 4: Vorfallsinformationen

Im nächsten Schritt wird der Angriff näher definiert (s. Abbildung 5). Hierbei wird zunächst durch Auswahl aus einer Dropdown-Liste definiert, welche Person bzw. welche Software auf den Angriff aufmerksam geworden ist. Wird eine Antwort ausgewählt, erscheint ein Freitext-Feld, in welchem detailliert beschrieben werden soll, wie diese Person oder Software den Angriff entdeckt hat. Als nächstes wird mithilfe der Autovervollständigung das vom Angriff betroffene Produkt (Software oder Hardware) und dessen Hersteller angegeben. Die Angabe des System sollte ursprünglich erst später im Formular gemacht werden. Bei der Implementierung der Website ist jedoch aufgefallen, dass die Abfrage nach CVE-Einträgen relativ viel Zeit in


1
Kontaktinformationen
2
Vorfallinformationen
3
Angriffsinformationen
4
Überprüfen
ANGRIFFSINFORMATIONEN
Hier haben Sie die Möglichkeit näher zu beschreiben wie der Angriff stattgefunden hat
Wie wurde der Angriff erkannt?
Beschreiben Sie bitte möglichst genau, wie der Angriff festgestellt wurde, sodass dieser Prozess für andere nachvollziehbar ist!
Wodurch ist der Angriff festgestellt worden?
Administrator
Können Sie genauer beschreiben, wie Administrator den Angriff festgestellt hat?
Wie kann der Angriff näher beschrieben werden?
Wenn einzelne Aspekte der Angriffsbeschreibung nicht eindeutig zu identifizieren sind, dann kreuzen Sie bitte alle in Frage kommenden Möglichkeiten an!
Welches System wurde angegriffen?
microsoft
windows 2000
windows 2000
windows 2000 advanced server
windows 2000 resource kit
windows 2000 terminal services
Wodurch wurde der Angriff ermöglicht?
Miskonfiguration:
Falsche Berechtigung
Veraltete Systemversion
Ungenutzte Features Aktiviert
Standardeinstellungen Beibehalten
USB Geräte (Speichermedien, Handy, etc.)
E-Mail (SPAM, Anhänge, etc.)
Unzureichende Eingabevalidierung:
Cross-Site Scripting
SQL Injection
Buffer Overflow
Criss-Site Request Forgery
Botnetz
Identitätsdiebstahl:
Man-In-The-Middle
Phishing
Spoofing
Pharming
Ausnutzen einer Sicherheitslücke eines IT-Produktes
Social Engineering
Sonstige Angaben
SCHADPROGRAMM: Schädlicher Code wurde infiltriert und wird auf dem betroffenen System ausgeführt.
DENIAL-OF-SERVICE: (D)DoS ist in der Regel die Folge einer Überbelastung eines Dienstes mithilfe eines Botnetzs.
BELIEBIGE CODEAUSFÜHRUNG: Der Angreifer hat sich auf eine Weise Zugang verschafft, welche ihn berechtigt beliebigen Code auf dem betroffenen System auszuführen.
Welche Art des Angriffes wurde ermöglicht?
Schadprogramm:
Virus
Wurm
Trojanisches Pferd
Adware
Spyware
Denial-of-Service
Beliebige Codeausführung
Sonstige Angaben
Welcher Zweck wurde durch den Angriff (vermutlich) verfolgt?
Erpressung
Identitätsdiebstahl
Entwendung vertraulicher Informationen
Störung der Geschäftstätigkeit
Sabotage / Denial-of-Service
Manipulation von Daten
Nutzung von Systemressourcen (Spam-Relay, Botnetz-Client, C&C-Server, Dropzone-Server)
Defacement
Sonstige Angaben

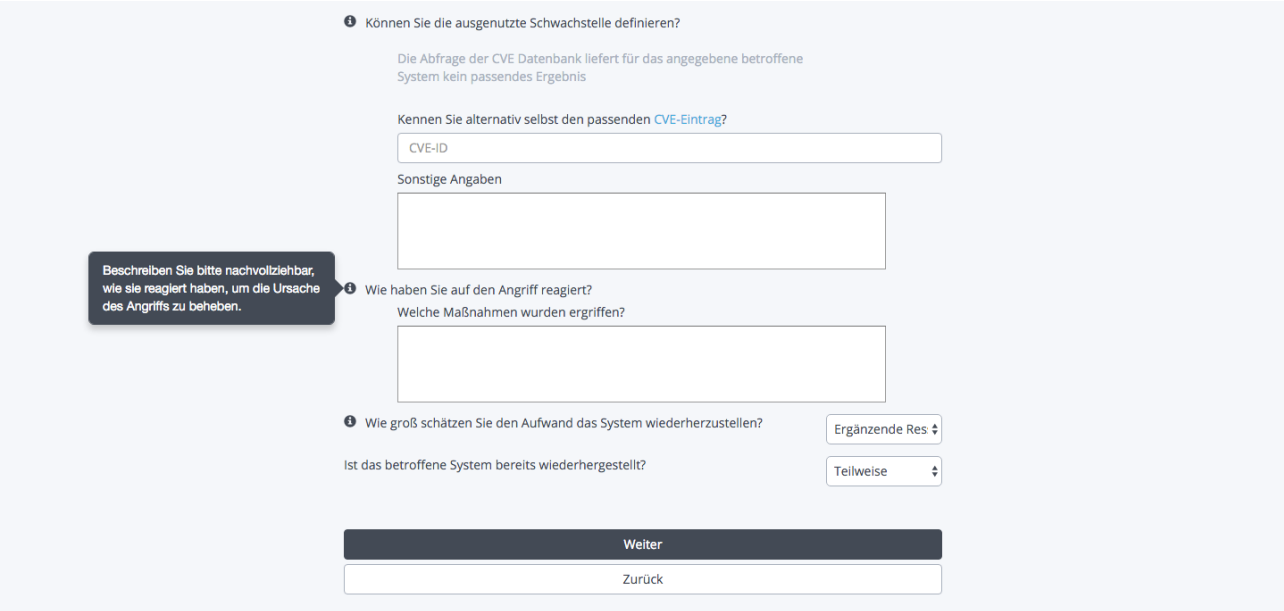


Abbildung 5: Angriffsinformationen

Anspruch nimmt. Es werden Hersteller und Produkt als Input dieser Abfrage daher schon möglichst früh angegeben, um Zeit zu gewinnen, bis der Nutzer die Stelle erreicht, an der er einen vorgeschlagenen CVE Eintrag auswählt. Sind Hersteller und Produkt aus der Liste der Autovervollständigung ausgewählt, wird als nächstes der Angriffsvektor beschrieben ("Wodurch wurde der Angriff ermöglicht?"). Hierzu werden die in Abschnitt 3 definierten Antwortmöglichkeiten als Auswahl von Checkboxen angeboten. Es ist eine Mehrfachauswahl möglich, da der Nutzer alle in Frage kommenden Möglichkeiten ankreuzen soll, wenn er sich nicht sicher auf eine Antwort festlegen kann. Einige Antwortmöglichkeiten ("Miskonfiguration", "Unzureichende Eingabevalidierung" und "Identitätsdiebstahl") können in einer nächsten Ebene detaillierter definiert werden. Hierzu können Badges an- und abgewählt werden. Außerdem hat der Nutzer über ein Freitext-Feld die Möglichkeit beliebige weitere Angaben bezüglich des Angriffsvektors zu machen. Auf gleiche Weise werden die kommenden Fragen nach der Art und dem Zweck des Angriffs beantwortet. Daraufhin wird nach der Schwachstelle des betroffenen Systems gefragt. Hierbei hat der Nutzer die Möglichkeiten einen der vorgeschlagenen CVE-Einträge auszuwählen, selbst einen CVE-Eintrag zu definieren und in einem Freitext-Feld tiefergehende Angaben zu machen. Ein weiteres Freitext-Feld wird im nächsten Schritt genutzt, damit der Nutzer beschreiben kann, wie er auf den Angriff reagiert hat. Außerdem werden hier durch Dropdown-Listen die in Abschnitt 3 definierten Antwortmöglichkeiten auf die Fragen "Wie groß schätzen Sie den Aufwand das System wiederherzustellen?" und "Ist das betroffene System bereits wiederhergestellt?" vorgegeben. Letztere Frage ist jedoch nur sichtbar, wenn der Nutzer die erste Frage mit "Vorhandene Ressourcen" oder "Ergänzende Ressourcen" beantwortet hat. Zu jeder Frage im Abschnitt "Angriffsinformationen" werden durch Info-Buttons tiefergehende Erläuterungen geliefert. Diese sind in Abbildung 5 beispielhaft dargestellt.

Als letzten Schritt des Meldeverfahrens zeigt Abbildung 6 eine Übersicht über die gemachten Angaben zum IT-Sicherheitsvorfall. Dem Nutzer wird eine übersichtliche Darstellung seiner Angaben präsentiert, damit er diese noch einmal auf Korrektheit und Vollständigkeit überprüfen kann. Des Weiteren wird an dieser Stelle die Meldeempfehlung ausgesprochen. Der Nutzer wird

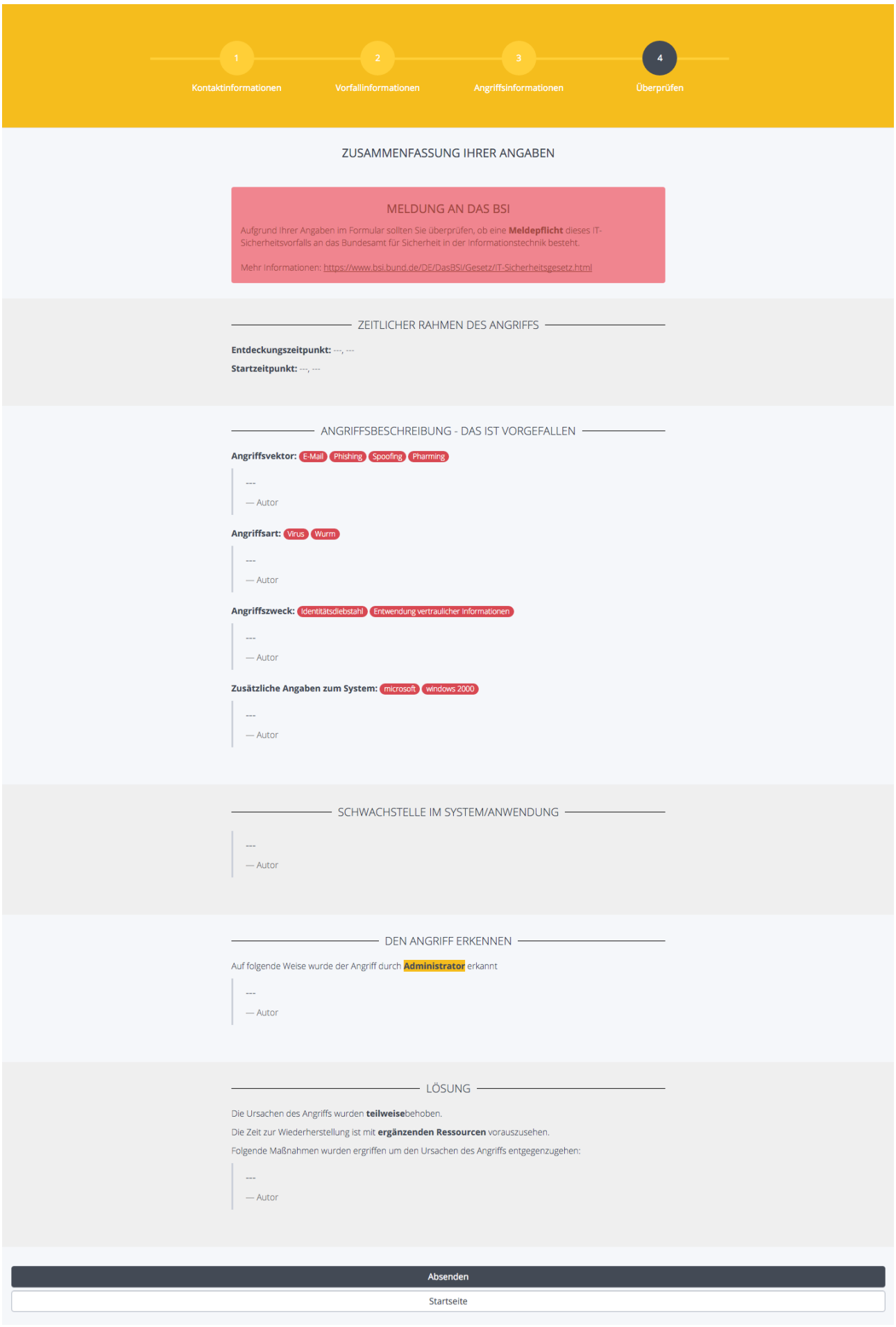


Abbildung 7: Übersicht über alle Angaben

darauf aufmerksam gemacht, dass der beschriebene Vorfall möglicherweise der Meldepflicht nach dem IT-Sicherheitsgesetz unterliegt. Dieses besagt, dass Betreiber kritischer Infrastrukturen Vorfälle mit "erheblichen" Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer Systeme an das BSI melden müssen. Daher wird eine Meldeempfehlung dann ausgesprochen wenn folgende Angaben im Formular gemacht werden:

- In Schritt 1 "Kontaktinformationen" wird die Frage ob man Betreiber einer kritischen Infrastruktur sei mit "Ja" beantwortet.
- In Schritt 2 "Vorfallsinformationen" wird die Frage nach der Höhe der funktionalen Auswirkungen mit "mittel" oder "hoch" beantwortet.

Wenn der Nutzer seine Angaben überprüft hat, kann er das Formular absenden, sodass es dauerhaft gespeichert und für andere zugänglich gemacht wird. Dies geschieht über eine Timeline. Immer wenn ein neuer IT-Sicherheitsvorfall gemeldet wird, wird dieser an oberster Stelle der Timeline dargestellt (s. Abbildung 8). Der Titel jedes Eintrags in der Timeline gibt an welches System betroffen wurde, da dies auf den ersten Blick die wichtigste Information ist, da man möglicherweise die gleiche Software oder Hardware benutzt und daher selbst gefährdet ist Opfer dieses Angriffs zu werden. Außerdem werden durch Tags auf übersichtliche Weise weitere Informationen zum Inhalt des hinterliegenden Angriffs gegeben.

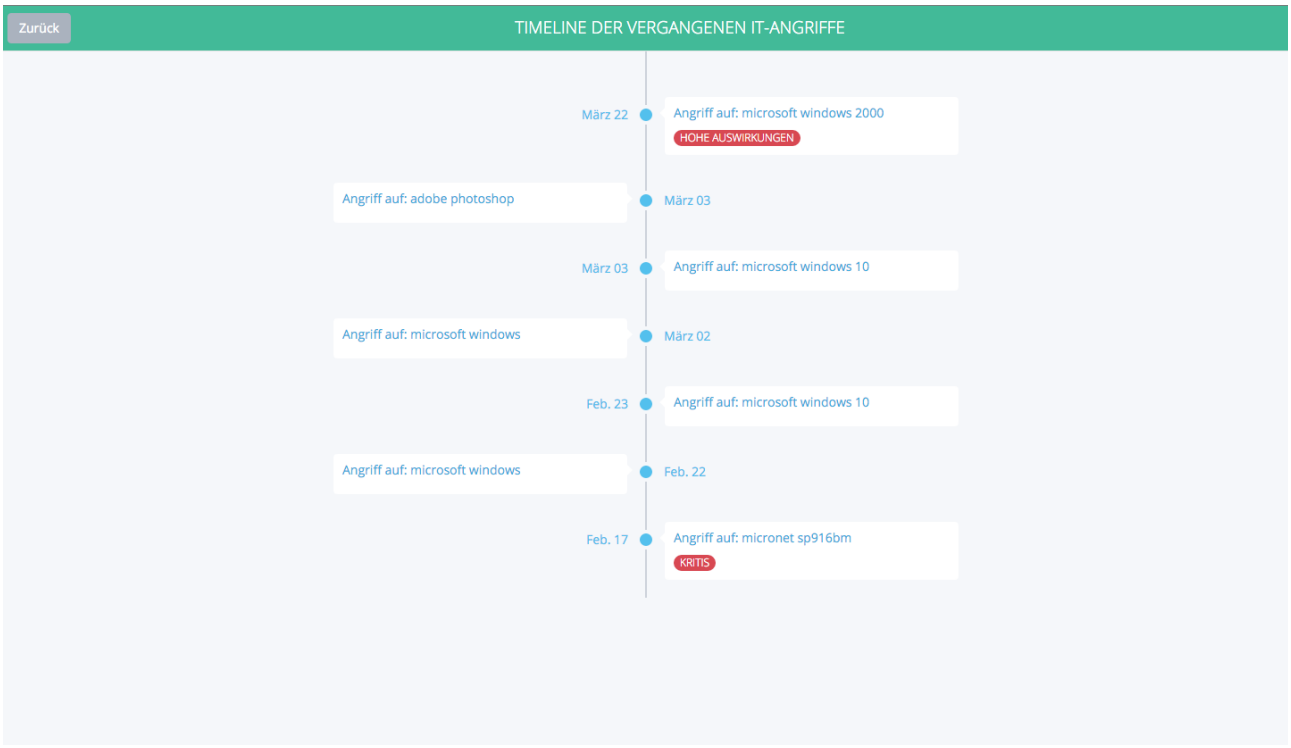


Abbildung 8: Timeline der IT-Sicherheitsvorfälle

Wird einer der Einträge aus der Timeline ausgewählt, erhält man eine detaillierte Zusammenfassung über den Angriff (s. Abbildung 9). Diese ist ähnlich aufgebaut, wie die Übersicht über die Angaben des Meldeformulars (Abbildung 7). Am unteren Ende der Angriffsdetails hat man die Möglichkeit über einen Button den Autor der Meldung direkt zu kontaktieren. Hierbei handelt es sich um einen mailto-Button, welcher den Email-Client öffnet, mit welchem eine Email an die vom Autor hinterlegte Email-Adresse gesendet werden kann.

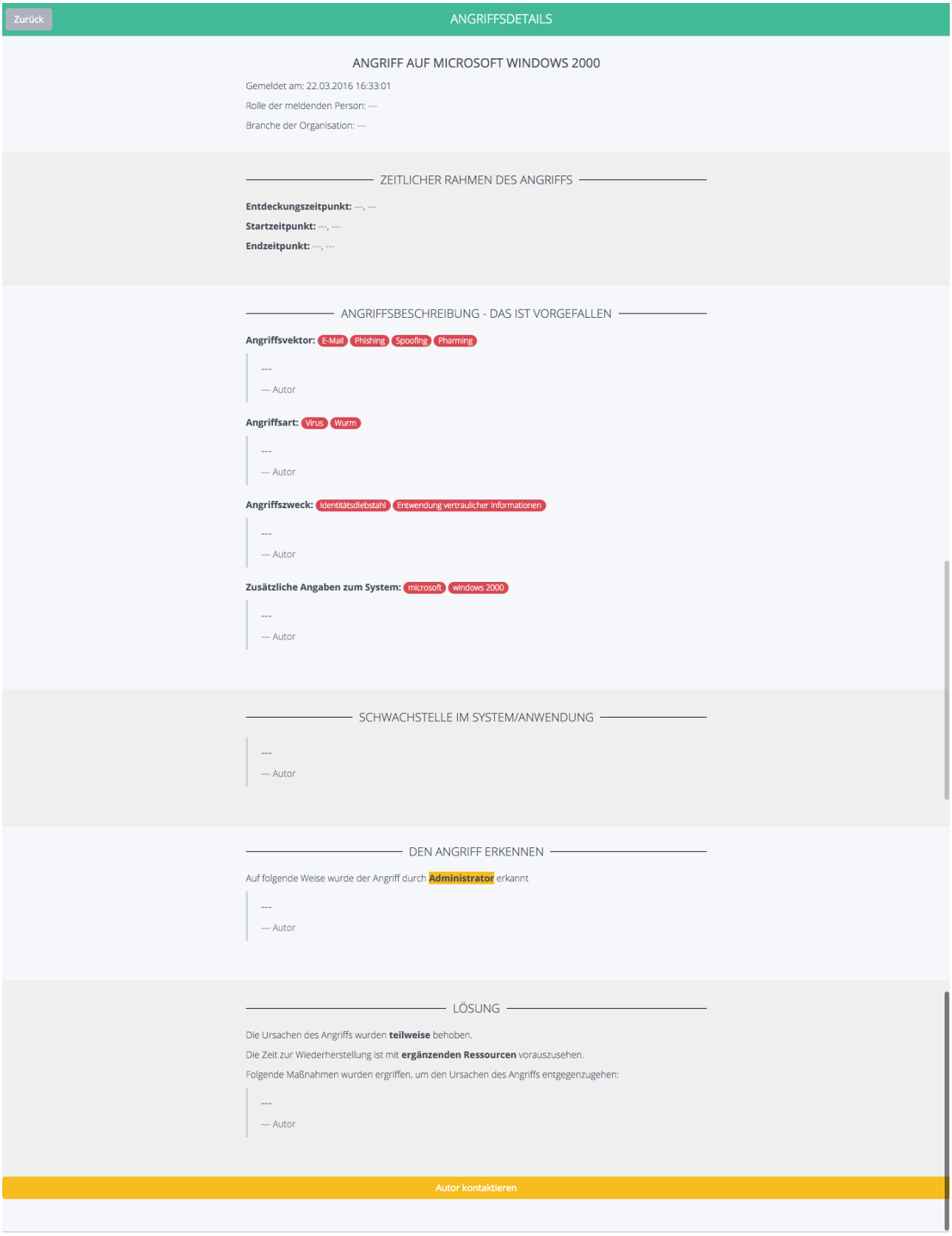


Abbildung 9: Angriffsdetails

5.1. Installationsanleitung

Im folgenden werden die einzelnen Schritte beschrieben, die notwendig sind um die einzelnen Softwarekomponenten zu installieren. Auf diese Weise sorgen die Paketverwaltungssysteme (NPM, Bower) dafür dass jeweils die Versionen der Frameworks und Plugins installiert werden, mit denen die Kompatibilität sichergestellt ist.

Für die Anbindung des Backends durch Baasbox[14] ist es notwendig dass Java 1.8 installiert ist. Ausserdem wird Node.js für den Paketmanager NPM und die API zur Autovervollständigung benötigt. Node.js kann unter https://nodejs.org heruntergeladen werden.

1. Der Code steht auf Github zur verfügung und kann, entsprechende Rechte vorausgesetzt, unter https://github.com/UniSiegenCSCW/ProjektarbeitITSicherheitsVorfaelle heruntergeladen werden.

2. Nachdem das Repository heruntergeladen und an eine entsprechende Stelle entpackt ist, wird mit dem Terminal zum Ordner *Frontend* gewechselt.

3. Zunächst muss das Grunt Command line interface[15] installiert werden. Dies geschieht über den Node Package Manager (NPM) und den Befehl:
   sudo npm install -g grunt-cli

4. Eine weitere Voraussetzung für die nächsten Schritte ist der Web-Paketmanager Bower[16] dieser wird ebenfalls per NPM installiert:
   sudo npm install -g bower

5. Durch Bower können jetzt alle notwendigen Frameworks automatisch installiert werden. Dazu muss im Ordner *Frontend* folgender Befehl eingegeben werden:
   bower install
   Hiermit werden alle Abhängigkeiten aus der Datei *bower.json* installiert.

6. Um alle Grunt Erweiterungen und Abhängigkeiten zu installieren, die insbesondere für den späteren Build notwendig sind, muss ebenfalls im Ordner *Frontend* der Befehl **npm install** ausgeführt werden.

7. Jetzt kann mit Hilfe von Grunt der Server gestartet werden, der die Webseite ausliefert. Sobald jetzt Änderungen am Code durchgeführt werden steht immer die aktuellste Version zur Verfügung. Der Server wird über **grunt serve** gestartet. Eine fertige Version, die auch auf einen Webserver übertragen werden kann, wird mit **grunt build** erzeugt.

8. Um die anfallenden Formulardaten zu speichern wird Baasbox verwendet. Nach der Installation muss diese zunächst über den Befehl **./start** (Mac OS) über das Terminal im Installationsverzeichnis gestartet werden.

---

[14] http://www.baasbox.com

[15] http://www.gruntjs.com

[16] http://www.bower.io

9. Jetzt kann sich über http://localhost:9000/ mit den Standard Daten
   Benutzername: **admin**
   Passwort: **admin**
   Appcode: **1234567890** eingeloggt werden.

10. Es muss zunächst ein neuer Benutzer mit
    Namen: **webapp**
    Passwort: **webapp**
    Role: **registered** angelegt werden.

11. Anschließend muss eine neue Collection mit dem Namen "**incidents**" angelegt werden.

12. Jetzt kann in den Ordner *API* im Terminal gewechselt werden und dort über den Befehl **node app.js** der Dienst zur Autovervollständigung der Softwarenamen gestartet werden.

13. Nun ist das Formular einsatzbereit und kann über http://localhost:9005/#/ aufgerufen werden.

5.2. Code-Strukturierung

Der Hauptordner *ProjektarbeitITSicherheitsVorfaelle* ist zunächst in die beiden Unterordner *API* und *Frontend* unterteilt. Der Ordner *API* beinhaltet die API zur Autovervollständigung und Abfrage der CVE-Einträge. Im Ordner *Frontend* ist die entwickelte Website abgelegt (siehe links). Der Unterordner *views* beinhaltet die einzelnen Seiten:

- **main.html**: Startseite
- **eins.html**: Schritt 1 des Meldeformulars (Kontaktinformationen)
- **zwei.html**: Schritt 2 des Meldeformulars (Vorfallsinformationen)
- **drei.html**: Schritt 3 des Meldeformulars (Angriffsinformationen)
- **fertig.html**: Schritt 4 des Meldeformulars (Übersicht über die Angaben
- **timeline.html**: Timeline der IT-Sicherheitsvorfälle
- **details.html**: Angriffsdetails über einen IT-Sicherheitsvorfall

Jede dieser HTML Seiten wird durch javascript-Controller gesteuert (*Frontend/app/scripts/controllers*). So greift **eins.html** beispielsweise auf Funktionen von **einsCtrl.js** zurück und analog bei anderen Seiten. Allen Controllern ist **superCtrl.js** übergeordnet, der das AngularJS-Model verwaltet, in welchem die Daten des Meldeformulars zwischengespeichert werden.

6. Fazit und Ausblick

Als Ergebnis dieser Projektarbeit steht ein vollfunktionsfähiger Prototyp zum digitalen Austausch von IT-Sicherheitsvorfällen bereit. Dabei wird besonderer Fokus auf den Gewinn von Informationen über vorgefallene Angriffe auf Informationstechnologie gelegt. Dieser erfolgt über ein Online-Meldeformular, welches von einem Mitglied einer Organisation ausgefüllt wird, welche von einem derartigen Angriff betroffen ist. Bei der Gestaltung des Formulars wird besonderer Wert darauf gelegt, dass der Meldeprozess weitestgehend automatisiert erfolgt, um dem Nutzer einerseits Aufwand zu ersparen, sodass die Hürde der Nutzung des Formulars geringer ist, und andererseits Vergleichbarkeit zwischen einzelnen Vorfallsmeldungen zu gewährleisten. Eine vollständige Automatisierung des Formulars ist jedoch wenig sinnvoll, da dem Nutzer so die Möglichkeit fehlen würde wichtige zusätzliche Angaben zu machen, welche den inhaltlichen Horizont des automatisierten Formulars überschreiten würden. Eine große Herausforderung bei der Entwicklung des Formulars ist also die Balance zwischen der Automatisierung der Angaben (Vorgabe von Antwortmöglichkeiten) und der Freiheit des Nutzers bei der Beantwortung von Fragen (durch Freitext-Felder). Eine weitere Schwierigkeit besteht darin die Expertise eines Nutzers im Bereich der IT-Sicherheit einzuschätzen. Hiervon ist abhängig, wie gut dieser die Geschehnisse eines Vorfalls beschreiben kann, bzw. wie viel Hilfestellung ihm dafür gegeben werden muss. Besonders bei Schritt 3 des Meldeformulars (Angriffsinformationen) ist diese Schwierigkeit deutlich erkennbar. Aus diesem Grund sollten zur Weiterführung des Ergebnisses dieser Projektarbeit zunächst Praxis- und Usability-Tests durchgeführt werden. Reale Nutzer müssten sich mit dem entwickelten Prototypen auseinandersetzen, damit festgestellt werden kann, ob die hier gewählte Vorgehensweise zur Meldung eines IT-Sicherheitsvorfalls praxistauglich ist oder nicht. Der inhaltliche Ablauf des Formulars beruht größtenteils auf Erkenntnissen der Wissenschaft und Best-Practices anderer Meldeformulare. Eine empirische Untersuchung auf Vollständigkeit, Korrektheit und Verständlichkeit der gewählten Vorgehensweise des Formulars ist daher notwendig.

Bei der Gestaltung des Formulars wurde über weitere Features diskutiert, welche durch die entwickelte Plattform unterstützt werden könnten. Da der Kern der Projektarbeit zunächst nur die grundlegende Entwicklung des Formulars und die Darstellung der darin gewonnenen Informationen ist, wurden diese bei der Implementierung nicht weiter einbezogen. Nennenswerte zusätzliche Features sind:

- **Nutzerverwaltung und Kommentarbereich**: Mithilfe einer Nutzerverwaltung der Plattform ist eine Kommentarfunktion im Bereich der Darstellung eines gemeldeten Vorfalls (Angriffsdetails) möglich. So müsste nicht der umständliche Weg der Email genutzt werden um Kontakt zum Autor der Meldung aufzunehmen und außerdem würden direkt auf der Plattform Diskussionen entstehen, welche für alle Nutzer nützlich sein könnten, um gemeinsam über Cyber-Angriffe zu lernen.

- **Mehrere Angriffe pro Vorfall**: Ein Vorfall kann als Abfolge von mehreren einzelnen Angriffen gesehen werden. Dies liegt beispielsweise dann vor, wenn aus Sicht des Angreifers verschiedene Systeme geknackt werden müssen, damit ein übergeordnetes Ziel erreicht wird. Für das Meldeverfahren wäre es dann sinnvoll diese einzelnen Angriffe, die ein gemeinsames

Ziel verfolgen, miteinander zu verknüpfen, damit sie alle zusammen als ein Vorfall betrachtet werden können.

- **Anbindung an das Meldeverfahren des BSI**: Hinsichtlich der ursprünglichen Motivation dieser Projektarbeit, dem Inkrafttreten des IT-Sicherheitsgesetz, wäre es sinnvoll die hier entwickelte Plattform mit dem Meldeverfahren des BSI zu verknüpfen. Dies könnte so aussehen, dass neben der Meldung innerhalb der Plattform eine weitere Meldung besipielsweise als PDF generiert wird, welche den Anforderungen des BSI entspricht und somit im nächsten Schritt dorthin übermittelt werden kann.