Kritische Erfolgsfaktoren für ein Computer Emergency Response Team (CERT)

Michael Kohler

Bachelor of Science in Computer Science
Fernfachhochschule Schweiz

Diese Arbeit ist Teil des Moduls
SEMA

October 2016

Abstract

Aufgabenstellung gemäss Dozenten-Themenliste des Moduls SEMA:

> “Ein Computer-Notfallteam oder auch Computer Emergency Response Team (CERT) trägt mit seiner Expertise zum Thema IT-Sicherheit massgeblich dazu bei, dass möglichen Angriffen auf IT-Infrastrukturen bereits im Vorfeld wirksam begegnet werden kann. Auch nach einem IT-Sicherheitsvorfall ist ein CERT bei der Wiederaufnahme des Regelbetriebs und der Ermittlung der Verursacher eine nahezu unverzichtbare Unterstützung. Diese Arbeit erläutert zunächst die notwendigen Grundlagen zum Verständnis eines CERTs undefasst sich danach intensiv mit der Fragestellung, anhand welcher Faktoren der Erfolg eines Computer- Notfallteams festgemacht werden kann und welche Punkte sowohl bei dessen Aufbau als auch dessen Betrieb beachtet werden sollten.“

Inhaltsverzeichnis

Abbildungsverzeichnis

Glossar

Acronyms / Abbreviations

CERT Computer Emergency Response Team

CSIRT Computer Security Incident Response Team

ENISA European Union Agency for Network and Information Security

GPG GNU Pretty Good Privacy

PEST Political, Economical, Social, Technological

SWOT Strengths, Weaknesses, Opportunities, Threats

TLD Top Level Domain

Kapitel 1

Grundlagen

1.1 Definition

Ein Computer Emergency Response Team (CERT) (Deutsch: "'Computer-Notfall-Team"') ist ein Team, welches sich um IT-Sicherheit kümmert. Es analysiert mögliche Bedrohungen und wirkt möglichen Angriffen und Bedrohungen bereits vor dem Eintreten entgegen. Sollte es trotzdem zu einem Angriff kommen, ist das CERT verantwortlich die Ursachen zu ermitteln, dagegen vorzugehen und unterstützt bei der Wiederaufnahme des Regelbetriebs massgeblich mit.

1.2 CERT und CSIRT

CERT Der Begriff "CERT" wurde vom Software Engineering Institute an der Carnegie Mellon University geprägt. Die CERT Devision arbeitet u.a. an der Forschung von Cybersecurity-Themen. Der Fokus liegt hierbei jedoch nicht nur auf der Forschung, sondern auch an der Entwicklung von Informationen zu IT-Sicherheitsthemen. Zusätzlich arbeitet die Devision auch mit Softwareherstellern, um die Sicherheit von Softwareprodukten zu erhöhen. [2] Die CERT Devision wurde im Jahre 1988 nach dem Auftreten des Morris-Wurms an der Carnegie Mellon University in Pittsburg, Pensylvania in den USA gegründet. [5] Finanziert wurde diese Gründung durch das amerikanische Department of Defense. In den USA ist der Begriff "'CERT"' markenrechtlich geschützt und gehört der Carnegie Mellon University.

CSIRT Aus diesem Grund werden CERT auch häufig als Computer Security Incident Responsive Team (CSIRT) bezeichnet. Es gibt jedoch auch einige Ausnahmen, wie z.B. der CERT-Bund des deutschen Bundesamtes für Sicherheit in der Informationstechnik.

In dieser Arbeit werde ich beide Begriffe verwenden, wobei ich CERT als Markenname und CSIRT als Konzeptbegriff verwende.

1.3 Grundlegende Aufgaben

Durch das schnelle Wachstum und die Popularität des Internets befinden sich viele Firmen sehr schnell im Visier von Cyberattacken. Fast alle Firmen haben schützenswerte Informationen in ihren Systemen, welche deshalb genügend geschützt werden müssen. Bedrohungen sind nicht zwingend nur E-Spionage oder Konkurrenz. Bedrohungen durch das Internet reichen von “normalen“ Viren und Ransomware [8] bis zum gezielten Eindringen in Computernetzwerke von Firmen, um Daten zu entwenden oder zerstören. Eine komplette Abschottung und Eliminierung aller Angriffsvektoren ist Utopie, daher muss hierfür ein Mittelweg gefunden werden.

Um diese Grundlage als CSIRT zu erfüllen, gehören folgende Aufgabenbereiche zum Tätigkeitsbereich eines CSIRTs:

- Analyse der Bedrohungslage
- Erkennung von Angriffen im Voraus
- Erkennung von momentanen Angriffen
- Elimierung von momentanen Angriffen
- Erarbeitung eines Notfallkonzeptes
- Sofortiges Eingreifen in einer Bedrohungslage und direkte Massnahmen zur Sicherung und Notfall-Betriebes von kritischen Geschäftsprozessen
- Unterstützung bei der Wiederaufnahme des Regelbetriebs
- Koordination mit anderen CSIRTs

1.4 Forum of Incident Response and Security Teams

Nachdem 1988 das erste CERT an der Cornegie Mellon University gegründet wurde, gründete sich 1990 der Dachverband “Forum of Incident Response and Security Teams“.

Die FIRST fördert die globale Zusammenarbeit zwischen Notfallteams und definiert “Best Practices“. Zudem werden Frameworks durch die FIRST zur Verfügung gestellt, welche den Aufbau und Betrieb von CERTs definieren, sowie auch Weiterbildungsmaterial um die globale Akzeptanz und das Wissen zu Security Incident Management zu fördern.

1.5 CERT in der Schweiz

Das bekannteste CERT in der Schweiz wird von SWITCH Information Technology Services gestellt. SWITCH ist verantwortlich für die .ch und .li Domains. Zusätzlich erbringt SWITCH auch Dienstleistungen im nationalen Forschung- und Bildungsnetzwerk und verlinkt Schweizer Universitäten mit anderen, internationalen Universitäten.

Dank des CERTs der SWITCH ist die Schweizer Top Level Domain (TLD) eine der sichersten der Welt und die sicherste TLD Europas. [7]

1.5.1 Gründung des SWITCH CERT

Die CERT-Abteilung von SWITCH existiert bereits seit 20 Jahren. 1994 wird der Aufbau einer Fachstelle für Sicherheitsfragen geschaffen. Gemäss Geschäftsbericht der SWITCH dieses Jahres werden bereits einige sicherheitsrelevante Anfragen von Kunden der SWITCH beantwortet und die SWITCH informierte über bekanntgewordene Sicherheitsverletzungen. Die Akkreditierung der SWITCH-CERT erfolgt 1996 durch das CERT/CC der CERT-Koordinationsstelle der Carnegie Mellon University.

1.6 CERT in Deutschland

Auch in Deutschland sind mehrere CERTs tätig. Neben dem CERT der Universität Stuttgart sowie dem CERT des deutschen Forschungsnetzwerkes hatte sich auch Mcert etabliert. Das Mcert richtete sich vorallem an kleine und mittlere Unternehmen. Mittlerweile existiert die Mcert nicht mehr und wird durch das neu erschaffene CERT-Bund weitergeführt.

1.6.1 CERT-Bund

CERT-Bund ist die CERT des Bundesamts für Sicherheit in der Informationstechnik (BSI).

"CERT-Bund hat das Ziel als zentrale Anlaufstelle für präventive und reaktive Maßnahmen mit Bezug auf sicherheits- und verfügbarkeitsrelevante Vorfälle in Computersystemen zu fungieren. IT-Sicherheitsvorfälle werden in Zusammenarbeit mit Betroffenen von CERT-Bund bearbeitet." [1]

Das CERT-Bund bietet unter anderem folgende Dienstleistungen an: 24-Stunden-Support, Betrieb eines Lagezentrums, Analyze von und Empfehlungen zu Vorfällen anhand von Meldungen, Warndienste, Alarmierung der Bundesverwaltung

1.6.2 Bürger-CERT

Da das CERT-Bund nicht alle Anliegen von Privaten bearbeiten kann, wurde eine separate CERT ins Leben gerufen. Dieses Projekt untersteht auch dem deutschen BSI. Privatpersonen sowie Unternehmen können sich kostenlos diverse Dienstleistungen wie z.B. Gefährdungsnewsletter und -Alarmierungen via E-Mail abonnieren. So können sich auch kleinere Unternehmen über die Gefahrenlage informieren und proaktiv nach der Alarmierung gegen Gefahren schützen.

1.7 Security Incident Management

Security Incident Management bezeichnet das Vorgehen, wie bei Bedrohungen der IT-Sicherheit vorgegangen werden muss. Dies involviert Monitoring und Erkennen von Bedrohungen in Computer oder Computer-Netzwerken. Tritt ein Incident (Event) ein, wird dieses gemäss definiertem Prozess effektiv behandelt. Wie ein solcher Prozess aussehen kann, wird später veranschaulicht.

Security Incident Management ist die Grundlage für CISRT. Ohne Definition, wie mit Security Incidents umgegangen werden soll, kann das Response Team nicht arbeiten. Security Incident Management ist eines der wichtigsten Teilgebiete der IT-Security und dadurch Teil der ISO-27000 Familie. ISO-27035 [4] definiert die Grundlagen für das Security Incident Management und definiert fünf Phasen.

1.7.1 Phase 1: Prepare

In der Vorbereitungsphase ist das Ziel ein CSIRT aufzubauen und die dafür benötigten Prozessgrundlagen zu erarbeiten. Sobald diese Prozesse und das Team definiert sind, kann mit dem Monitoring von Bedrohungen und Identifizieren von Incidents fortgeführt werden.

Wichtige Fragen:

- Wie soll auf ein Incident reagiert werden?
- Wer reagiert wie und wann?
- Wie ist der Eskalationsprozess aufgebaut?
- Wie setzt sich das Response Team zusammen?
- Wer wird wann informiert?
- Wo werden Incidents dokumentiert?
- Wie werden Incidents in Zukunft vermieden?

1.7.2 Phase 2: Identify

In der Identifikationsphase geht es darum, dass Bedrohungen und Incidents schnell und korrekt identifiziert werden können. Sobald ein Incident identifiziert wird, muss dieser sofort gemäss Prozessdefinition gemeldet werden. Je nach Prozess kann dies in verschiedenen Tools gemeldet werden. Ein Beispiel dafür wäre ein Ticket beim Service Desk. Hierbei ist es wichtig, dass die korrekte Prioriät übernommen wird und nicht innerhalb der anderen Tickets untergeht.

Der ISO-27035-Standard definiert Vorlagen für das Reporting von Security Incidents. Diese dürfen entsprechend verwendet werden und können, falls nötig, auch an die eigene Unternehmensstruktur angepasst werden.

1.7.3 Phase 3: Assess

In der Assess-Phase wird ermittelt, wie mit diesem Incident vorgangen werden kann.

Fragen, die sich das CSIRT stellen muss in dieser Phase beinhalten unter anderem:

- Muss das System offline genommen werden bis der Incident behoben ist?
- Müssen forensische Daten gesammelt werden, bevor das System wieder funktionstüchtig gemacht werden kann?
- Reicht es aus, das System zu patchen und wieder online zu bringen?
- Muss das System komplett neu aufgesetzt werden?

1.7.4 Phase 4: Respond

Sind die möglichen Optionen klar und die beste(n) davon gewählt, muss der Incident behoben werden. Die definierten Aktionen werden durchgeführt bis das System wieder im Normalbetrieb ist. Ist dies erledigt, kann der Incident geschlossen werden.

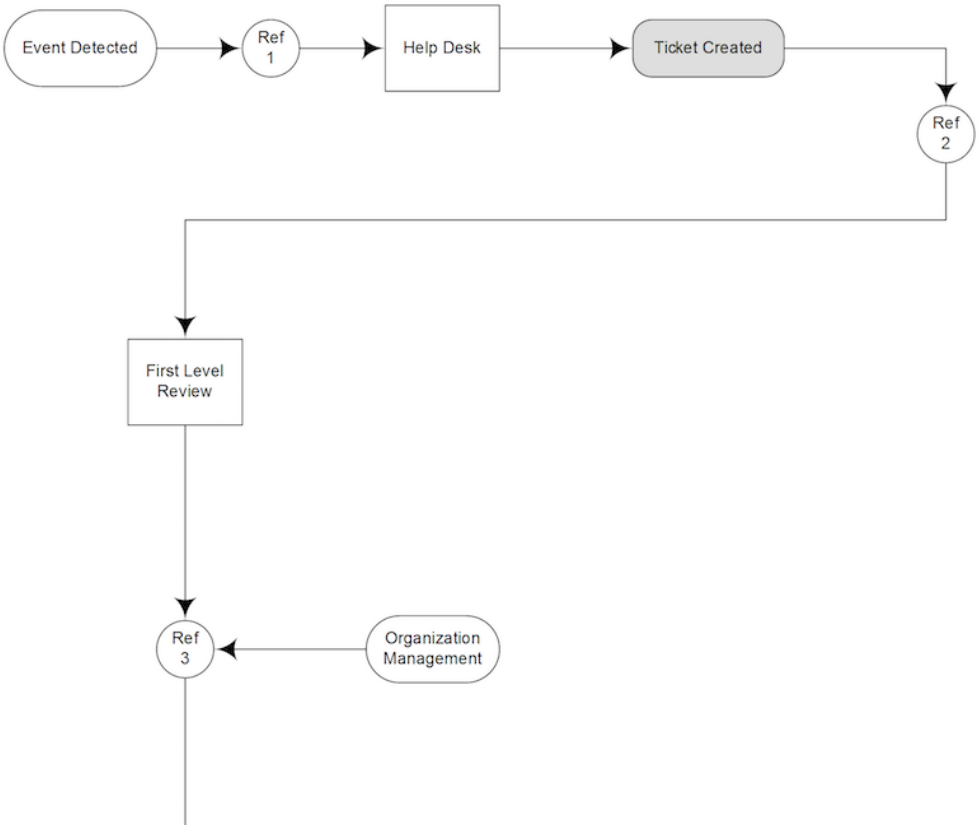

Abbildung 1.1 Auszug aus einem Security Incident Management Workflow. Image: CC-BY 2.5, Autor: Michael Berman

1.7.5 Phase 5: Learn

Der Incident ist zwar gelöst, aber der Prozess ist noch nicht fertig angewendet. Phase 5 definiert "Lessions learnt". Um in der Zukunft besser und effektiver auf einen Incident zu reagieren, werden die durch diesen Incident gewonnenen Erkenntnisse analysiert und dokumentiert. Nur so kann sichergestellt werden, dass sich das CSIRT mit den Erkenntnissen auseinandersetzt und diese dazu verwendet, den Prozess zu optimieren. Da ein Prozess nie perfekt ist, sollten diese Erkenntnisse in die Prozessoptimierung einfliessen. Dabei ist es wichtig, dass dies regelmässig gemacht wird, damit der Prozess immer möglichst effektiv und effizient abgearbeitet werden kann.

Kapitel 2

Aufbau und Betrieb eines CERT

2.1 Aufbau

Da die Effizienz ein Grundbaustein eines CERT ist, muss bereits der Aufbau vorsichtig geplant werden. Dieser Teil der Arbeit orientiert sich am "CSIRT Setting up Guide"der ENISA. [3]

Die ENISA ist die European Union Agency for Network and Information Security. Die Aufgabe der ENISA ist es, die erforderliche hochgradige Netz- und Informationssicherheit in der EU zu gewährleisten. Dafür berät sie die Behörden der EU-Staaten sowie EU-Institutionen zur Netz- und Informationssicherheit. Zudem dient sie als Forum für den Austausch bewährter Verfahren sowie als Kontakt zwischen EU-Institutionen, Behörden und Unternehmen.

2.1.1 Analyse der Klientel

Bevor der Geschäftsplan ausgearbeitet werden kann, müssen die Anforderungen der Kunden (“Klientel“ hat sich im CERT-Umfeld als Ausdruck dafür etabliert) genau analysiert werden. Da CERT in verschiedenen Szenarien eingesetzt werden können, ist dies ein wichtiger Schritt. Auch das Umfeld des Klientels hat eine grosse Auswirkung auf die Planung des CERTs sowie auf dessen Betriebsmodus.

Hierbei spielt es keine Rolle, ob die Klientel intern ist (z.B. bei einem CERT für eine bestimmte Unternehmung) oder mehrere Organisationen oder die Öf-

fentlichkeit umfasst. Sind die Anforderungen und Erwartungen nicht klar genug beim Aufbau, besteht eine hohe Chance bereits zu Beginn der Betriebsphase zu scheitern, da die Prozesse den Kundenbedürfnissen nicht entsprechen.

Grundsätzlich können hierfür alle Methodiken des Anforderungsmanagements (Require Engineering) und des Planungsmanagements verwendet werden. Der ENISA Guide erwähnt hierzu folgende zwei Analyse-Werkzeuge, die ich nochfolgend kurz erleutern werde:

- SWOT-Analyse
- PEST-Analyse

SWOT

Bei der SWOT-Analyse werden die Stärken, Schwächen, Chancen und Gefährdungen (engl. Strength, Weakness, Opportunities, Threads) analyisert. Dabei sind Stärken und Schwächen interne Punkte. Diese werden gegenüber anderer Anbieter (auch "Konkurrenten") analysiert. Dies ergibt eine Übersicht, wie sich die Kunden im Markt positiert haben und wo interne Verbesserungschancen erkannt werden können. Chancen und Gefährdungen werden als externe Punkte betrachtet. Hierbei wird auf die Umgebung geachtet und Punkte aufgenommen, welche vom Kunden zum eigenen Nutzen gemacht werden können, bzw. den Kunden bedrohen.

PEST

Bei der PEST-Analyse ist das Ziel, die politische, ökonomische, soziokulterelle und technologische Umfeld des Kunden zu verstehen. Dies ist eine reine Umfeld-Analyse und interne Punkte werden nicht aufgelistet.

Da in den meisten Fällen bei der Analyse der Kunden für ein CSIRT sowohl interne wie auch externe Faktoren wichtig sind, bietet es sich an eine SWOT- und eine PEST-Analyse zu machen. So kann von Anfang an sichergestellt werden, dass nicht bereits bei der Planung des CSIRT in die falsche Richtung optimiert wird.

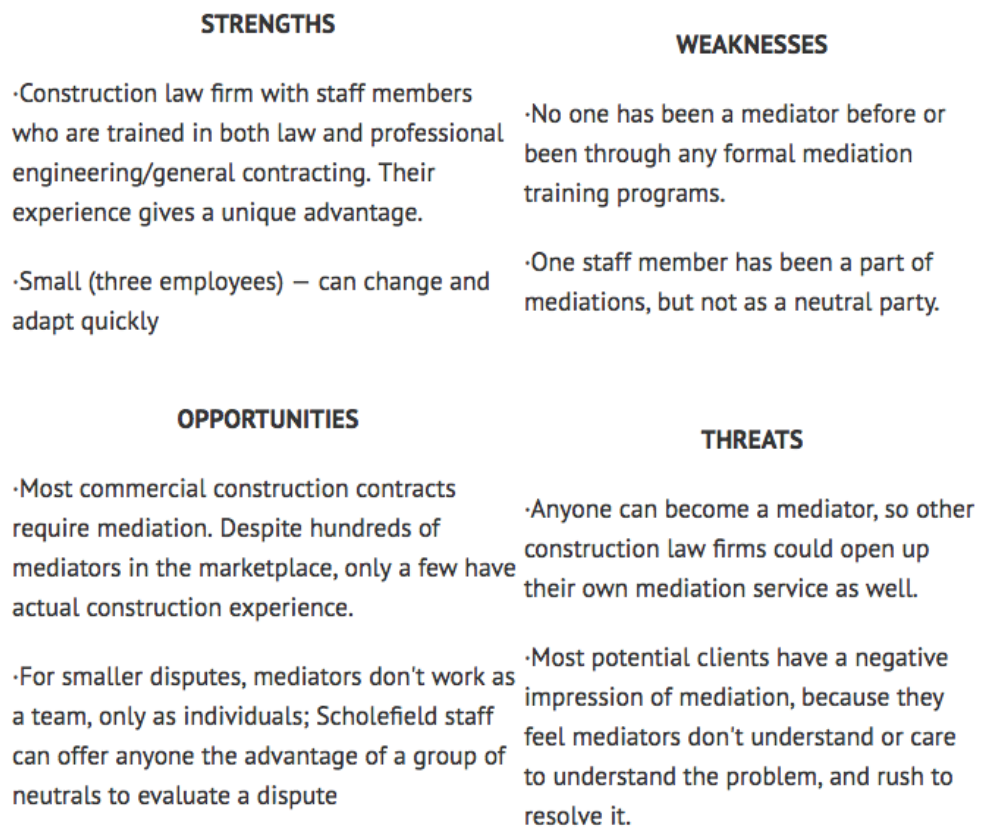

Abbildung 2.1 Beispiel einer SWOT-Analyse. Quelle: http://www.businessnewsdaily.com/4245-swot-analysis.html

2.1.2 Festlegen des Aufgabenbereichs

Als nächstes muss der Aufgabenbereich des CSIRT definiert werden. Dies sollte eine möglichst kurz und knappe Formulierung sein, da diese der Grundstein des CSIRT ist und im besten Fall über Jahre hinweg Gültigkeit hat und nicht angepasst wird. Generell werden diese Formulierungen allgemein gehalten und enthalten keine spezifischen, prozessbedingten Angaben.

2.1.3 Ausarbeitung des Geschäftsplans

Nachdem der Aufgabenbereich definiert wurde, werden spezifischere Angaben im Geschäftsplan gemacht.

Finanzierung

Oft ist in der Praxis die Finanzierung an ein bestimmtes Budget geknüpft. Die wichtigsten Faktoren sind die Dienstzeiten sowie die Anzahl Personenstellen, die für das CSIRT arbeiten.

Dem gegenüber steht ein mögliches Ertragsmodell. Hierbei kommt es darauf an, an welche Kundenbedürfnisse sich das CSIRT richtet. Ist das CSIRT z.B. für die öffentliche Hand, sind Subventionen und Gelder vom Staat eine Option. Eine andere Option ist ein Mitgliedermodell mit Zusatzertrag gemäss Aufwand für Zusatzdienste z.B. Sicherheitsaudits.

Organisation und Einstellen von Mitarbeitern

Es gibt verschiedene Organisationsmodelle, die für ein CSIRT in Frage kommen. Entweder kann die CSIRT als eigenständige Organisation fungieren (d.h. mit eigener Geschäftsleitung etc.) oder kann als Team innerhalb einer bestehenden Organisation aufgebaut werden. Bei einer verteilten Organisation kann auch in Betracht gezogen werden, aus allen Standorten eine Person zu verpflichten. In der Praxis ist es schwierig, die genau erforderliche Anzahl Mitarbeiter zu bestimmen. Die ENISA spricht von mindestens vier Vollzeitstellen für das Verteilen von Security Advisories und Behandlung von Vorfällen. Übernimmt die CSIRT weitere Verantwortungen und muss z.B. Schichtdienst leisten, spricht die ENISA von mindestens 12 Vollzeitstellen. Hier gilt es die definierten Aufgabengebiete zu

analysieren und die Kundenbedürfnisse korrekt zu analysieren. Eine Koordination mit anderen CSIRT kann von Vorteil sein, um z.B. eine 24/7 Abdeckung zu erhalten, bedingt aber das Lösen von anderen logistischen Herausforderungen.

Richtlinien für die Informationssicherheit

Je nach Kundentyp differenzieren die zu erstellenden Richtlinien zur Informationssicherheit. Es werden die betrieblichen sowie die administrativen Abläufe und Prozesse definiert. Wichtig dabei ist, dass nationale Richtlinien und Gesetze angewendet und befolgt werden. Viele Länder verfügen z.B. über Datenschutzgesetze, welche von allen eingehalten werden müssen. Ausserdem müssen Richtlinien definiert werden, die z.B. besagen wie Informationen klassifiziert und veröffentlicht werden. Grundsätzlich ist es zu empfehlen Security Advisories öffentlich zugänglich zu machen. Schwachstellen in Kunden-Systemen dürfen z.B. nicht vor dessen Behebung veröffentlicht werden. Eine genaue Spezifikation der Abläufe und Klassifikationen hilft dabei keine Kunden zu verärgern oder Gesetze zu missachten. Hier ist es auch wichtig die Geschäftsleitung mit einzubeziehen, damit organisationsweite Richtlinien mit eingebracht werden können. Natürlich sollte die Geschäftsleitung im gesamten Prozess mindestens “informiert“ (siehe RASCI [6]) sein. In den meisten Fällen ergibt es jedoch Sinn, die Geschäftsleitung möglichst früh und eng einzubinden.

2.2 Betrieb

Nachfolgend werde ich einige Beispiele von Betriebsfällen nennen und erläutern, was dabei zu beachten ist.

2.2.1 Analyse von Klienten

Um für das Klientel die wichtige Aufgabe eines CSIRT auszuführen, ist es unabdingbar sich von der Umgebung der Klienten ein Bild zu machen. Dabei wird ein genaues Inventar geführt, welche Software bei welchen Kunden im Einsatz ist. Nur so kann effektiv informiert werden, falls eine Sicherheitslücke gefunden wird und entsprechend die Lage beurteilt werden. Wichtig dabei ist, dass diese auch aktuell gehalten wird, da ansonsten Warnungen gesendet werden, welche

den Kunden gar nicht mehr betreffen. Dies dient zudem als Grundlage für alle weiteren Fälle.

2.2.2 Alarme und Warnungen

Anhand der oben erstellen Software-Liste können aktuelle und akute Sicherheits- und Bedrohungswarnungen an die Kunden gesendet werden. Hierbei gilt es zu beachten, dass nur Meldungen an Kunden gesendet werden, welche tatsächlich auch von dieser Vulnerability betroffen sind. Ansonsten führt das schnell zu einer "Geht mich ja nichts an"-Wahrnehmung und die Kunden werden entsensibilisiert, was genau das Gegenteil des Zweckes einer CSIRT ist. Damit der Kunde die Bedrohung entsprechend einschätzen kann, ist es zu bevorziehen jeweils auch eine Analyse der Auswirkung des Incidents zu errechnen. Hierbei bedeutet die Auswirkung die Eintrittswahrscheinlichkeit multipliziert mit dem Risiko.

Wichtig ist auch jeweils eine Empfehlung (z.B. Patch einspielen) für jedes Bulletin rauszugeben, damit die Kunden genau wissen, wie sie die Bedrohungslage verringern können. Zusätzlich ist es wichtig, dass diese Nachrichten durch den Kunden als vertrauenswürdig eingestuft werden können. Hierfür kann z.B. E-Mail-Signierung via GPG verwendet werden.

2.2.3 Schulungen

Ein weiterer, sehr wichtiger Punkt sind regelmässige Schulungen. Die IT-Landschaft und dessen Bedrohungen und Gefahren ändern sich fast täglich. Es ist wichtig, dass Angestellte immer auf dem aktuellsten Stand der Informationen sind, damit diese Kunden ihr Wissen entsprechend weitergeben können.

Eine Sensibilisierung der Kunden ist genauso wichtig. Wenn ein Kunde zwar die Meldung erhält, dass es eine Bedrohung der IT-Sicherheit gibt, diese aber ignorieren, bzw. entgegen der Empfehlung als "unwichtig" einstufen, kann dies zu gravierenden Problemen führen. Daher ist es auch wichtig, Schulungen für Kunden zu veranstalten, um diese zu sensibilisieren.

Kapitel 3

Erfolgsfaktoren eines CERT

3.1 Aufbau - Kritische Erfolgsfaktoren

3.1.1 Einsatz von Ressourcen (Mitarbeiter, Zeit, Budget)

Wie bei jedem Projekt muss sichergestellt werden, dass verfügbare Ressourcen korrekt und effektiv eingesetzt werden. Dabei sind sinnvolle Methodiken des Projektmanagementes anzuwenden. Mitarbeiter-Ressourcen, ihre verfügbare Zeit sowie auch das Budget sind hierbei die wichtigsten Faktoren. So muss z.B. sichergestellt werden, dass genügend Ressourcen vorhanden sind, jedoch ein Leerlauf möglichst verhindert wird. Hierbei gilt es jedoch darauf zu achten, dass der Einsatz von Ressourcen vernünftig ist. “So wenig wie möglich“ ist hierbei der falsche Ansatz und führt zu mangelhafter Qualität.

Im Vergleich zu anderen Erfolgsfaktoren sind diese mit gängigen Projektmanagement-Methoden messbar.

3.1.2 Projektabschluss

Analog zum Einsatz der Ressourcen ist bei Projekten auch der zeitlich vereinbarte Projektabschluss-Termin wichtig. Mit den angemessenen Projektplanungsmethoden kann die Wahrscheinlichkeit eines zu späten Abschlusses reduziert werden. Hierbei ist wichtig, dass mögliche Verspätungen schnellstmöglich kommuniziert werden, damit die Projektdauer entsprechend abgeschlossen werden kann. Verzögert sich der Abschluss des Projektes zu lange, besteht das Risiko,

dass sich die Umgebung geändert hat und nicht mehr alle Bedürfnisse abgedeckt werden können. Eine zu grosse Fokussierung auf “wir müssen das Projekt sofort abschliessen“ hindert jedoch die Umsetzung von qualitativ hochwertigen Ergebnissen.

3.1.3 Unterstützung durch das Management

Für beide oben genannten Erfolgsfaktoren ist es unabdingbar, dass das Management Unterstützung bietet. Es müssen Ressourcen geplant und Budget investiert werden. Schlussendlich sind dies Entscheidungen des Managements. Somit ist es wichtig, das Management frühzeitig und stetig in den Prozess des Aufbaus einzubinden und wo nötig zu konsultieren. In jedem Fall sollte das Management über den Projektstand regelmässig informiert werden.

3.1.4 Kundenglaubwürdigkeit

Falls das Aufbau-Projekt von Kunden finanziert wird und nicht rein interner Natur ist, ist auch die Glaubwürdigkeit gegenüber der Kunden ein wichtiger Erfolgsfaktor. Der Kunde muss sicher sein, dass das aufzubauende Team in der Lage ist die gewünschten Dienstleistungen für die Kunden zu übernehmen. Hierbei ist z.B. wichtig, dass regelmässig über den Projektfortschritt kommuniziert wird, da auch im Betrieb des CSIRT schlussendlich Kommunikation einer der wichtigsten Bestandteile sein wird. Wird bereits während des Projektes nicht genügend kommuniziert, deutet dies auf eine Schwachstelle des Teams hin und es könnte davon ausgegangen werden, dass dies sich auch im Betrieb nicht ändern wird. Auch gegenüber Kunden, welche sich nicht finanziell am Projekt beteiligen, sollte regelmässig kommuniziert werden. Schlussendlich müssen die Kunden sicher sein, dass das Team ihre Anforderungen gewissenhaft, korrekt und zeitkritisch umsetzen kann.

3.1.5 Bestehende Ressourcen / Hilfe von anderen CERTs

Ein weiterer Erfolgsfaktor sind bestehende Ressourcen, bzw. Hilfe von anderen Teams. Soweit bestehende Ressourcen genutzt werden können, sollte auch darauf zugegriffen werden. Im CERT-Bereich sind viele Informationen öffentlich

zugänglich. Diese sollten bereits beim Aufbau analysiert und eingebunden werden, da so das bestmögliche Ergebnis erreicht werden kann.

Andere CERT können beim Aufbau wesentlich zur Qualität beitragen, da diese sich bereits im Betriebsstadium befinden und ggf. wichtige “Lessions learned“ vermitteln können.

3.2 Betrieb - Kritische Erfolgsfaktoren

Beim Betrieb kommen fast die selben Kategorien von Erfolgsfaktoren zum Einsatz, da viele der Faktoren auch weiterhin gültig sind.

3.2.1 Einsatz von Ressourcen (Mitarbeiter, Zeit, Budget)

Auch während des Betriebs muss sichergestellt werden, dass genügend Ressourcen vorhanden sind. Ein unterbesetztes CSIRT kann nicht die geforderten Leistungen erbringen und senkt somit die Kundenzufriedenheit. Wie in jeder anderen Organisation muss jedoch auch sichergestellt werden, dass die vorhandenen Ressourcen auch nach Projektabschluss vernünftig eingesetzt werden.

3.2.2 Unterstützung durch das Management

Die Unterstützung des Managements ist weiterhin wichtig. Obwohl nach Projektabschluss ggf. ein Jahres-Budget vorhanden ist, muss wie bei jeder anderen Organisation auch, darauf geachtet werden, dass Änderungen der Managementstrategie in Einklang mit den Zielen des CSIRT gebracht werden. Ein kontinuierlicher Austausch zwischen Management und dem CSIRT-Team ist unabdingbar.

3.2.3 Angebotene Dienstleistungen / Kundenzufriedenheit

Erst während des Betriebs kann ermittelt werden, ob die angeboten Dienstleistungen den Kundenanforderungen entsprechen oder sich diese mittlerweile in eine andere Richtung bewegt haben. Die Kundenzufriendenheit betreffend Reaktionszeit, Qualität und Beratung kann z.B. mittels eines Fragebogens regelmässig überprüft werden. Zudem sollte regelmässig eine Analyse der Kunden

(mit SWOT oder PEST) durchgeführt werden, um sicherzustellen, dass die angebotenen Dienstleistungen weiterhin die bestmögliche Qualität aufweisen. Dies ist einer der wichtigsten Faktoren für den Betrieb, da ohne Kunden (extern sowie auch intern) das Team nicht mehr benötigt wird und Dienstleistungen von anderen Anbietern angefordert werden.

3.2.4 Dokumentation

Um die Qualität und Zufriendeheit auf einem hohen Niveau zu halten, muss die Dokumentation immer wieder aktualisiert werden und allfällige "Lessions learned" angewendet werden. Nur so ist es möglich eine kontinuierlich hohe Qualität zu leisten und die Prozesse weiter zu verbessern. Die Dokumentation jedes Falles in einem ausreichenden Mass kann in Zukunft sehr wertvoll sein, auch wenn dies im ersten Augenblick nicht der Fall zu schein mag. Die Dokumentation hilft auch dabei neuen Mitarbeitern den Einstieg leichter zu machen und bereits vorhandenes Wissen zu vermitteln.

3.2.5 Bestehende Ressourcen / Hilfe von anderen CERTs

Während des Betriebs kann weiterhin auf die Mithilfe von anderen CERTs sowie auch auf den Zugriff von bestehenden Ressourcen gezählt werden. Je besser die Zusammenarbeit mit anderen Teams funktioniert, desto besser können die Kunden in ihren Anforderungen unterstützt und kompetent bedient werden.

Literaturverzeichnis

[1] CERT-Bund (2016). Cert-bund – das computer-notfallteam des bsi. [online] https://www.cert-bund.de/about. Abgerufen am 08.10.2016.

[2] CERT Devision (2016). About us | the cert divison. [online] https://www.cert.org/about/. Abgerufen am 15.10.2016.

[3] enisaguide (2006). Enisa - csirt setting up guide. [online] https://www.enisa.europa.eu/publications/csirt-setting-up-guide. Abgerufen am 12.10.2016.

[4] iso27035 (2011). Iso/iec 27035. [online] http://www.iso27001security.com/html/27035.html. Abgerufen am 08.10.2016.

[5] NetworkWorld (2015). Certs and cirts: homonyms but not synonyms, part 1. [online] http://www.networkworld.com/article/2328305/lan-wan/certs-and-cirts--homonyms-but-not-synonyms--part-1.html. Abgerufen am 08.10.2016.

[6] rasci (2016). Responsibility assignment matrix. [online] https://en.wikipedia.org/wiki/Responsibility_assignment_matrix#RASCI. Abgerufen am 15.10.2016.

[7] SWITCH (2016). Die switch-cert-story. [online] http://www.switch.ch/de/stories/20years_cert/. Abgerufen am 08.10.2016.

[8] Trend Micro USA (2016). Ransomware definition. [online] http://www.trendmicro.com/vinfo/us/security/definition/ransomware/. Abgerufen am 08.10.2016.