

DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle

1. Beschreibung

1.1. Einleitung

Bei Advanced Persistent Threats (APT) handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen. Dabei verschafft sich ein Angreifer dauerhaften Zugriff zu einem Netz und weitet diesen Zugriff auf weitere IT-Systeme aus. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und umfassende technische Fähigkeiten auf Seiten der Angreifer aus. Angriffe dieser Art sind in der Regel schwierig zu detektieren.

Nachdem ein APT-Angriff entdeckt wurde, stehen die Verantwortlichen in den betroffenen Institutionen vor großen Herausforderungen. Denn sie müssen eine Bereinigung durchführen, die über das übliche Vorgehen zur Behandlung von IT-Sicherheitsvorfällen hinausgeht. Es ist davon auszugehen, dass die entdeckten Angreifer bereits seit längerer Zeit auf die betroffene IT-Infrastruktur zugreifen können. Außerdem nutzen sie komplexe Angriffswerkzeuge, um die Standard-Sicherheitsmechanismen zu umgehen und diverse Hintertüren zu etablieren. Zudem besteht die Gefahr, dass die Angreifer die infizierte Umgebung genau beobachten und auf Versuche zur Bereinigung reagieren, indem sie ihre Spuren verwischen und die Untersuchung sabotieren.

In diesem Baustein wird von einer hohen Bedrohungslage durch einen gezielten Angriff hochmotivierter Täter mit überdurchschnittlichen Ressourcen ausgegangen. In der Praxis ist es üblich, dass bei einem solchen Vorfall immer auch ein (zertifizierter) Forensikdienstleister hinzugezogen wird, wenn die Institution selbst nicht über entsprechende eigene Forensik-Experten verfügt. Forensik-Dienstleister werden dabei bereits in der Phase der forensischen Analyse herangezogen. Die Dienstleister werden jedoch auch bei der Bereinigung zumindest beratend einbezogen.

1.2. Zielsetzung

Dieser Baustein beschreibt, wie eine Institution vorgehen sollte, um nach einem APT-Angriff die IT-Systeme zu bereinigen und den regulären und sicheren Betriebszustand des Informationsverbunds wiederherzustellen.

1.3. Abgrenzung und Modellierung

Der Baustein DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle* ist immer dann anzuwenden, wenn nach einem APT-Vorfall die IT-Systeme bereinigt werden sollen, um den regulären und sicheren Betriebszustand eines Informationsverbunds wiederherzustellen. Der Baustein ist auf den Informationsverbund anzuwenden.

Ein Informationsverbund kann nur bereinigt werden, wenn der APT-Vorfall vorher erfolgreich detektiert und forensisch analysiert wurde. Detektion und Forensik sind jedoch nicht Thema dieses Bausteins. Diese Themen werden in den Bausteinen DER.1 *Detektion von sicherheitsrelevanten Ereignissen* bzw. DER.2.2 *Vorsorge für die IT-Forensik* behandelt.

Im vorliegenden Baustein geht es ausschließlich um die Bereinigung von APT-Vorfällen. Andere Vorfälle werden im Baustein DER.2.1 *Behandlung von Sicherheitsvorfällen* behandelt. Auch beschreibt der Baustein nicht, wie sogenannte Indicators of Compromise (IOCs), also Einbruchsspuren, abzuleiten sind und wie diese benutzt werden können, um wiederkehrende Angreifer zu erkennen. Ebenso wird nicht darauf eingegangen, wie sich eventuell bei der Analyse und Bereinigung übersehene Hintertüren finden lassen.

Es werden ausschließlich Cyber-Angriffe berücksichtigt. Das heißt, es werden keine Angriffe betrachtet, mit denen sich Angreifer z. B. physischen Zugriff auf den Informationsverbund verschaffen. So werden Angriffsformen, bei denen in Rechenzentren eingebrochen, Administratoren bestochen, neu beschaffte Hardware abgefangen und manipuliert oder elektromagnetische Strahlung abgehört werden, nicht in diesem Baustein betrachtet.

Bereinigen Forensik-Dienstleister die IT-Systeme ganz oder teilweise, gelten die Anforderungen dieses Bausteins auch für diese Dienstleister. Durch vertragliche Vereinbarungen und Prüfungen kann dabei sichergestellt werden, dass sich die Dienstleister auch daran halten (siehe OPS.2.1 *Outsourcing für Kunden*).

2. Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle* von besonderer Bedeutung.

2.1. Unvollständige Bereinigung

APT-Angreifer wollen üblicherweise einen Informationsverbund dauerhaft infiltrieren. Sie verfügen über die dafür notwendigen Ressourcen und sind in der Lage, langfristige Angriffskampagnen durchzuführen. Dafür benutzen sie Werkzeuge und Methoden, die auf ihr Angriffsziel abgestimmt sind. Auch wenn ein APT-Vorfall entdeckt wird, kann nicht davon ausgegangen werden, dass sämtliche Zugangswege der Angreifer gefunden, alle Infektionen und Kommunikationswege von Schadsoftware beseitigt und alle Hintertüren entfernt wurden. Bei einer unvollständigen Bereinigung ist es jedoch sehr wahrscheinlich, dass ein Angreifer zu einem späteren Zeitpunkt, z. B. nach einer längeren Ruhephase, erneut auf die IT-Systeme zugreift und seinen Zugang wieder ausbaut. Das kann er beispielsweise, indem er Hintertüren nicht nur in Betriebssystemen und Anwendungssoftware platziert, sondern auch hardwarenahe Komponenten wie etwa Firmware manipuliert. Solche Modifikationen sind sehr schwer zu identifizieren und das notwendige Wissen, um sie zu extrahieren und zu analysieren, ist nur wenig verbreitet. Versuchen die Zuständigen z. B. die IT-Komponenten zu bereinigen, indem sie die Firmware überschreiben oder aktualisieren, kann es trotzdem passieren, dass der Angreifer auch die Update-Routinen modifiziert hat. Auf diesem Weg kann er dann wieder auf die IT-Systeme zugreifen.

2.2. Vernichtung von Spuren

Nach einem APT-Vorfall werden IT-Systeme oft neu installiert oder ganz ausgemustert. Wurde jedoch zuvor von den IT-Systemen keine forensische Kopie angefertigt, können Spuren vernichtet werden, die für eine weitere Aufklärung des Vorfalls oder sogar für ein Gerichtsverfahren notwendig wären.

2.3. Vorzeitige Alarmierung des Angreifers

Üblicherweise wird vor der Bereinigung eines APT-Vorfalles der Angriff über längere Zeit hinweg beobachtet und forensisch analysiert, um so alle Zugangswege sowie die verwendeten Werkzeuge und Methoden zu identifizieren. Bemerkt der Angreifer während dieser Phase, dass er entdeckt wurde, greift er eventuell zu Gegenmaßnahmen. Beispielsweise kann er versuchen, seine Spuren zu verwischen, oder er sabotiert noch weitere IT-Systeme. Auch könnte er den Angriff zunächst abbrechen oder weitere Hintertüren einrichten, um den Angriff später fortzuführen.

Da bei einem APT-Angriff grundsätzlich davon ausgegangen werden muss, dass die gesamte IT-Infrastruktur der Institution kompromittiert wurde, ist das Risiko hoch, dass der Angreifer die Bereinigungsaktivitäten entdeckt. Das gilt insbesondere, wenn die kompromittierte IT-Infrastruktur benutzt wird, um die Bereinigung zu planen und zu koordinieren. Finden die wesentlichen Schritte zur Bereinigung nicht in der korrekten Reihenfolge statt oder werden kritische Maßnahmen nicht gleichzeitig und aufeinander abgestimmt durchgeführt, erhöht sich die Gefahr, dass der Angreifer alarmiert wird. Isolieren die Zuständigen beispielsweise das Netz schrittweise statt auf einmal, wird der Angreifer eventuell gewarnt, bevor sein Zugriff effektiv beendet ist.

2.4. Datenverlust und Ausfall von IT-Systemen

Bei der Bereinigung eines APT-Vorfalles werden verschiedene IT-Systeme neu installiert und auch Netze temporär isoliert. Dadurch fallen zwangsweise IT-Systeme aus und Dienste sind damit z. B. nur noch eingeschränkt oder gar nicht mehr verfügbar. Dauert die Bereinigung sehr lange, kann dadurch die Produktivität der Institution ausfallen. Das kann wiederum signifikante wirtschaftliche Einbußen zur Folge haben, die sogar existenzbedrohend sein können. Dies ist insbesondere dann der Fall, wenn keine oder keine ausreichende Dokumentation für einen Wiederaufbau verfügbar ist.

2.5. Fehlender Netzaufbau nach einem APT-Angriff

Bei einem APT-Angriff erlangt der Angreifer detaillierte Kenntnisse darüber, wie die Zielumgebung aufgebaut und konfiguriert ist. Zum Beispiel kennt er die existierenden Netzsegmente, Namensschemata für IT-Systeme, Benutzer- und Dienstkonten sowie eingesetzte Software und Services. Durch dieses Wissen kann sich derselbe Angreifer unter Umständen auch nach einer Bereinigung erneut Zugang zur Zielumgebung verschaffen. Er kann sich sehr gezielt, effizient und unauffällig innerhalb des Netzes bewegen und in kurzer Zeit erneut einen hohen Infektionsgrad erreichen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle* vorrangig erfüllt werden:

DER.2.3.A1 Einrichtung eines Leitungsgremiums (B)

Um einen APT-Vorfall zu bereinigen, MUSS ein Leitungsgremium eingerichtet werden, das alle notwendigen Aktivitäten plant, koordiniert und überwacht. Dem Gremium MÜSSEN alle für die Aufgaben erforderlichen Weisungsbefugnisse übertragen werden.

Wenn ein solches Leitungsgremium zu dem Zeitpunkt, als der APT-Vorfall detektiert und klassifiziert wurde, bereits eingerichtet ist, SOLLTE dasselbe Gremium auch die Bereinigung planen und leiten. Wurde schon ein spezialisierter Forensik-Dienstleister hinzugezogen, um den APT-Vorfall zu analysieren, SOLLTE dieser auch bei der Bereinigung des Vorfalls miteinbezogen werden.

Ist die IT zu stark kompromittiert, um weiter betrieben zu werden, oder sind die notwendigen Bereinigungsmaßnahmen sehr umfangreich, SOLLTE geprüft werden, ob ein Krisenstab eingerichtet werden soll. In diesem Fall MUSS das Leitungsgremium die Bereinigungsmaßnahmen überwachen. Das Leitungsgremium MUSS dann dem Krisenstab berichten.

DER.2.3.A2 Entscheidung für eine Bereinigungsstrategie (B)

Bevor ein APT-Vorfall tatsächlich bereinigt wird, MUSS das Leitungsgremium eine Bereinigungsstrategie festlegen. Dabei MUSS insbesondere entschieden werden, ob die Schadsoftware von kompromittierten IT-Systemen entfernt werden kann, ob IT-Systeme neu installiert werden müssen oder ob IT-Systeme inklusive der Hardware komplett ausgetauscht werden sollen. Weiterhin MUSS festgelegt werden, welche IT-Systeme bereinigt werden. Grundlage für diese Entscheidungen MÜSSEN die Ergebnisse einer zuvor durchgeführten forensischen Untersuchung sein.

Es SOLLTEN alle betroffenen IT-Systeme neu installiert werden. Danach MÜSSEN die Wiederanlaufpläne der Institution benutzt werden. Bevor jedoch Backups wieder eingespielt werden, MUSS durch forensische Untersuchungen sichergestellt sein, dass dadurch keine manipulierten Daten oder Programme auf das neu installierte IT-System übertragen werden.

Entscheidet sich eine Institution dagegen, alle IT-Systeme neu zu installieren, MUSS eine gezielte APT-Bereinigung umgesetzt werden. Um das Risiko übersehener Hintertüren zu minimieren, MÜSSEN nach der Bereinigung die IT-Systeme gezielt daraufhin überwacht werden, ob sie noch mit dem Angreifer kommunizieren.

DER.2.3.A3 Isolierung der betroffenen Netzabschnitte (B)

Die von einem APT-Vorfall betroffenen Netzabschnitte MÜSSEN vollständig isoliert werden (Cut-Off). Insbesondere MÜSSEN die betroffenen Netzabschnitte vom Internet getrennt werden. Um den Angreifer effektiv auszusperrern und zu verhindern, dass er seine Spuren verwischt oder noch weitere IT-Systeme sabotiert, MÜSSEN die Netzabschnitte auf einen Schlag isoliert werden.

Welche Netzabschnitte isoliert werden müssen, MUSS vorher durch eine forensische Analyse festgelegt werden. Es MÜSSEN dabei sämtliche betroffenen Abschnitte identifiziert werden. Kann das nicht sichergestellt werden, MÜSSEN alle verdächtigen sowie alle auch nur theoretisch infizierten Netzabschnitte isoliert werden.

Um Netzabschnitte effektiv isolieren zu können, MÜSSEN sämtliche lokalen Internetanschlüsse, z. B. zusätzliche DSL-Anschlüsse in einzelnen Subnetzen, möglichst vollständig erfasst und ebenfalls berücksichtigt werden.

DER.2.3.A4 Sperrung und Änderung von Zugangsdaten und kryptografischen Schlüsseln (B)

Alle Zugangsdaten MÜSSEN geändert werden, nachdem das Netz isoliert wurde. Weiterhin MÜSSEN auch zentral verwaltete Zugangsdaten zurückgesetzt werden, z. B. in Active-Directory-Umgebungen oder wenn das Lightweight Directory Access Protocol (LDAP) benutzt wurde.

Ist der zentrale Authentisierungsserver (Domaincontroller oder LDAP-Server) kompromittiert, MÜSSEN sämtliche dort vorhandenen Zugänge gesperrt und ihre Passwörter ausgetauscht werden. Dies MÜSSEN erfahrene Administratoren umsetzen, falls erforderlich, auch mithilfe interner oder externer Forensikexperten.

Wurden TLS-Schlüssel oder eine interne Certification Authority (CA) durch den APT-Angriff kompromittiert, MÜSSEN entsprechende Schlüssel, Zertifikate und Infrastrukturen neu erzeugt und verteilt werden. Auch MÜSSEN die kompromittierten Schlüssel und Zertifikate zuverlässig gesperrt und zurückgerufen werden.

DER.2.3.A5 Schließen des initialen Einbruchswegs (B)

Wurde durch eine forensische Untersuchung herausgefunden, dass der Angreifer durch eine technische Schwachstelle in das Netz der Institution eingedrungen ist, MUSS diese Schwachstelle geschlossen werden. Konnten die Angreifer die IT-Systeme durch menschliche Fehlhandlungen kompromittieren, MÜSSEN organisatorische, personelle und technische Maßnahmen ergriffen werden, um ähnliche Vorfälle künftig zu verhindern.

DER.2.3.A6 Rückführung in den Produktivbetrieb (B)

Nachdem das Netz erfolgreich bereinigt wurde, MÜSSEN die IT-Systeme geordnet in den Produktivbetrieb zurückgeführt werden. Dabei MÜSSEN sämtliche zuvor eingesetzten IT-Systeme und installierten Programme, mit denen der Angriff beobachtet und analysiert wurde, entweder entfernt oder aber in den Produktivbetrieb überführt werden. Dasselbe MUSS mit Kommunikations- und Kollaborationssystemen erfolgen, die für die Bereinigung angeschafft wurden. Beweismittel und ausgesonderte IT-Systeme MÜSSEN entweder sicher gelöscht bzw. vernichtet oder aber geeignet archiviert werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle*. Sie SOLLTEN grundsätzlich erfüllt werden.

DER.2.3.A7 Gezielte Systemhärtung (S)

Nach einem APT-Angriff SOLLTEN alle betroffenen IT-Systeme gehärtet werden. Grundlage hierfür SOLLTEN die Ergebnisse der forensischen Untersuchungen sein. Zusätzlich SOLLTE erneut geprüft werden, ob die betroffene Umgebung noch sicher ist.

Wenn möglich, SOLLTEN IT-Systeme bereits während der Bereinigung gehärtet werden. Maßnahmen, die sich nicht kurzfristig durchführen lassen, SOLLTEN in einen Maßnahmenplan aufgenommen und mittelfristig umgesetzt werden. Der ISB SOLLTE den Plan aufzustellen und prüfen, ob er korrekt umgesetzt wurde.

DER.2.3.A8 Etablierung sicherer, unabhängiger Kommunikationskanäle (S)

Es SOLLTEN sichere Kommunikationskanäle für das Leitungsgremium und die mit der Bereinigung beauftragten Mitarbeiter etabliert werden. Wird auf Kommunikationsdienste Dritter zurückgegriffen, SOLLTE auch hier darauf geachtet werden, dass ein sicherer Kommunikationskanal ausgewählt wird.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

DER.2.3.A9 Hardwaretausch betroffener IT-Systeme (H)

Es SOLLTE erwogen werden, nach einem APT-Vorfall die Hardware komplett auszutauschen. Auch wenn nach einer Bereinigung bei einzelnen IT-Systemen noch verdächtiges Verhalten beobachtet wird, SOLLTEN die betroffenen IT-Systeme ausgetauscht werden.

DER.2.3.A10 Umbauten zur Erschwerung eines erneuten Angriffs durch denselben Angreifer (H)

Damit derselbe Angreifer nicht noch einmal einen APT-Angriff auf die IT-Systeme der Institution durchführen kann, SOLLTE der interne Aufbau der Netzumgebung geändert werden. Außerdem SOLLTEN Mechanismen etabliert werden, mit denen sich ein wiederkehrender Angreifer schnell detektieren lässt.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat folgende Dokumente zum Themenfeld APT veröffentlicht:

- BSI-Veröffentlichungen zur Cyber-Sicherheit (BSI-CS 072): „Erste Hilfe bei einem APT-Angriff“
- Common Criteria Protection Profile for Remote-Controlled Browsers Systems (ReCoBS): BSI-PP-0040

Das CERT-EU hat das weiterführende Dokument „CERT-EU Security Whitepaper 2014-007: Kerberos Golden Ticket Protection: Mitigating Pass-the-Ticket on Active Directory“ zum Themenfeld APT veröffentlicht.

5. Anlage: Kreuzreferenztablelle zu elementaren Gefährdungen

Die Kreuzreferenztablelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tablelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle* von Bedeutung.

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen