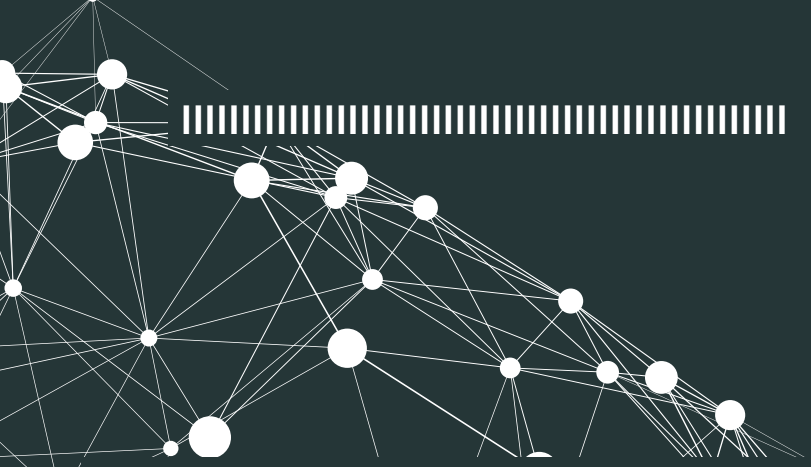

INCIDENT HANDLING PLAN

sure[secure]

00 INHALT

FÜR UNS IST SECURITY NICHT NUR EINE IDEE.

ES IST UNSERE LEIDENSCHAFT.

01 INCIDENT HANDLING

Meldungen über IT-Sicherheitsvorfälle gehören heutzutage leider zum Alltag. Ein bekannter Angriff ist zum Beispiel die Attacke auf den Filehoster des Online-Entwicklungsprojekts GitHub. Am 28. Februar 2018 brachen 1,35 Terabit Daten pro Sekunde auf den Server ein – die bisher größte DDos-Attacke. Solche Angriffe zielen darauf ab, dass Betreiber ihre Services vom Netz nehmen müssen. Im August 2013 wurden bei einem erfolgreichen Phishing-Angriff auf Yahoo die Konten von knapp einer Milliarden User kompromittiert. Solche Angriffe kosten Unternehmen Zeit und Geld und manchen Menschen sogar das Leben. Bei einem Cyberangriff auf das Seitensprungportal Ashley Madison im Jahre 2015 wurde gedroht, neben Namen und Adressen der Mitglieder, auch intime Informationen und Fotos zu veröffentlichen. Daraufhin nahm sich ein User das Leben.

Viele Unternehmen sind jedoch kaum oder gar nicht auf einen solchen Ernstfall vorbereitet. Dabei ist das schnelle Handeln in diesen Situationen essenziell. Dauert die Fehlerbehandlung aufgrund von mangelndem, internen Know-how zu lange, besteht das Risiko eines weiteren Datenverlustes und wachsenden oder sogar irreparablen Schadens.

Heutzutage muss leider nicht geklärt werden ob, sondern wann ein Angriff stattfinden wird. Ein gut geschultes Computer Incident Response Team (CIRT) ist in der Lage schnell auf einen Incident zu reagieren, den Schaden so gering wie möglich zu halten und die Sicherheit wiederherzustellen.

Dieses Nachschlagewerk soll als Hilfestellung dienen, damit im Ernstfall schnell reagiert werden kann. Die einzelnen Phasen aus Planung, Kommunikation und Durchführung bauen aufeinander auf und bieten die Grundlage einen eigenen Notfallplan erstellen zu können. Wichtig: Ein eigener Notfallplan benötigt Kapazitäten. Sollten Sie nicht genügend zur Verfügung stehen haben, ist es ratsam, einen externen Dienstleister zur Unterstützung zu beauftragen.

Die suresecure steht Ihnen jederzeit als Ansprechpartner zur Verfügung.

02 VORBEREITUNGEN

Ein Incident kann durch unterschiedlichste Störungen verursacht werden: von Stromausfällen über Hardwarefehler oder menschlichem Fehlverhalten bis hin zu gezielten Angriffen von Hackern. Die Vorbereitungsphase ist die wichtigste aller Phasen und beinhaltet folgende Planungspunkte:

GRÜNDUNG EINES CIRTS:

Das Computer Incident Response Team sollte aus Personen verschiedenster Bereiche zusammengestellt werden: IT-Mitarbeiter mit Spezialisierung, Rechtsanwälte, Mitarbeiter der Personalabteilung, Vertreter der Öffentlichkeitsarbeit, etc. Die unterschiedlichen Berufsfelder steigern das Fachwissen des Teams, erweitern die Fähigkeiten und ermöglichen das Reagieren auf Incidents auf verschiedene Arten.

TRAINING DES CIRTS:

Ein regelmäßiges Training des CIRTs gewährleistet die kurzfristige und schnelle Reaktion auf einen Incident. Durch die Schulung ist jedes Teammitglied in der Lage Strategien für verschiedene Sicherheitsvorfälle zu entwerfen und umzusetzen. Das Training mit dem gesamten Team fördert zudem die Zusammenarbeit im Umgang mit kritischen Situationen und stärkt die Notfallkompetenzen.

ACCESS CONTROL:

Das CIRT muss über alle erforderlichen Berechtigungen verfügen. Ein Netzwerk- oder Systemadministrator hat die Befugnis, im Rahmen eines Incidents, dem CIRT die Zugriffsrechte auf alle notwendigen Konten zu erlauben und diese nach Beseitigung des Incidents wieder zu entziehen. Es ist also ratsam, den Administrator schon im Vorfeld zu benennen.

02

DOKUMENTATION:

Ausführliche Dokumentationen erhöhen bei Störungen den Sicherheitsfaktor. Bei Fällen, die ein rechtliches Vorgehen erfordern, ist die Verwendung der ausführlichen Dokumentation des Incidents als Beweismittel von Vorteil.

LESSONS LEARNED:

Jegliche Aktionen, wie z. B. eingegebene Befehle, betroffene Systeme etc. sind zu dokumentieren, um Unklarheiten beim Formatieren von Festplatten und Neuinstallationen von Betriebssystemen auf einem Produktionsserver zu beseitigen.

BACK UPS

Die regelmäßige Durchführung von Backups wichtiger Systeme sichert die Wiederherstellung dieser im Bedarfsfall. In gleichmäßigen Intervallen durchgeführte Disaster Recovery Checks stellen sicher, dass die Backups auch wirklich funktionieren.

RICHTLINIE

Eine Richtlinie ist eine Zusammenfassung von Prinzipien, Regeln oder Methoden innerhalb eines Unternehmens und gibt einen Überblick darüber, ob ein Incident stattgefunden hat. Ein Login Banner weist autorisierte und legitime Benutzer auf ihre Verpflichtungen im Zusammenhang mit der ordnungsgemäßen Nutzung der Arbeitsumgebung hin. Weiter noch warnt es mögliche Eindringlinge vor illegalen Handlungen.

02

PRIORISIERUNG:

Ein Must-have für die Erstellung eines Reaktionsplans ist die vorherige Priorisierung von Incidents. Handelt es sich bei einem Security Incident nur um einen Netzwerkausfall, um ein Eindringen von außen oder den Befall mit Malware?

Die Priorisierung von Incidents sollte anhand der folgenden Fragen individuell für jedes Unternehmen erfolgen:

- Wie schnell schreitet der Incident voran?
- Welche Prozesse sind betroffen?
- Welche Auswirkungen haben die Angriffe?
- Ist eine weitere Ausbreitung möglich?
- Wie zeitkritisch sind die Aufgaben, die von Mitarbeitern nicht erfüllt werden können?
- Wie viele Kunden sind betroffen?
- Wie groß ist der finanzielle Schaden?
- Sind Menschenleben in Gefahr?

KOMMUNIKATIONSPLAN:

Ein Kommunikationsplan dient als Nachschlagewerk für das CIRT: WER muss WANN und WARUM kontaktiert werden? Auch das Management muss im gesamten Verlauf auf dem neuesten Stand gehalten werden. Informieren Sie unverzüglich Ihren externen Dienstleister und fordern Sie Hilfe an. Das Incident Response Team der suresecure steht Ihnen zeitnah zur Verfügung und unterstützt Sie dabei alle Schritte des Incident Handlings schnell und korrekt durchzuführen. So gelingt es Ihnen den Schaden zu minimieren.

Wichtig: Legen Sie im Vorfeld fest, in welchen Fällen die Polizei mit einbezogen werden sollte.

02

HILFSMITTEL:

Alle benötigten Hilfsmittel für einen Incident sollten in einem forensischen „Jump Bag“ aufbewahrt werden. Empfehlungen für den Inhalt:

- Incident Handling-Analyse-Ablaufplan (Wer mach was?)
- Kontaktliste der Teammitglieder
- Dokumentationen der Umgebung, Berechtigungen und Netzwerkpläne
- Bootfähiges USB-Medium, um initial nach Malware zu suchen
- Benötigte Soft- und Hardwareprodukte
- Notebooks mit Paketanalysesoftware, Treibern undandere Tools
- Werkzeugkasten
- Etikettier- und Dokumentationskit
- Set zur Beweissicherung
- Checklisten
- Kontaktdaten der sure[secure]: **IT-Notfallnummer: +49 (0) 2156 9749 110**

Das CIRT sollte jederzeit Zugriff auf den „Jump Bag“ haben.

03 IDENTIFIKATION

In dieser Phase gilt es zu prüfen, ob ein gemeldeter Systemausfall oder seltsames Verhalten eines Systems tatsächlich sicherheitsrelevant ist. Hierfür sollten zwei Administratoren unterschiedliche Quellen wie Log-Dateien, Fehlermeldungen, Intrusion Detection Systeme und Firewalls untersucht werden. Können Beweise für einen Incident identifiziert werden, sollte das CIRT umgehend informiert werden, um genügend Beweise zu sammeln und sich auf die nächsten Schritte vorzubereiten. Ohne die hinreichende Identifikation werden alle weiteren Maßnahmen nutzlos.

Alle Daten müssen sorgfältig dokumentiert werden, da diese Unterlagen für eine strafrechtliche Verfolgung des Täters verwendet werden können. Sollten die zuständigen Personen nicht in der Lage sein, den Grund für Anomalien oder Systemausfälle zu identifizieren, sollte ein externer Dienstleister hinzugezogen werden. Diese Phase zu Überspringen könnte im Ernstfall dazu führen, nicht alle Eintrittspunkte des Angreifers schließen zu können, da sie nicht alle identifiziert werden konnten.

Die suresecure bietet nicht nur einen Incident Response Service. Unter der Notfallnummer +49 (0) 2156 9749 110 können auch spontan Vorfälle gemeldet und Hilfe angefordert werden.

04 ISOLIERUNG

Alle Schritte dieser Phase sind notwendig, um einen Incident vollständig einzudämmen und die Vernichtung von Beweisen zu verhindern. Vor der weitergehenden Analyse des Sicherheitsvorfalles müssen die betroffenen Systeme zur Vermeidung weiterer Ausbreitung und Schäden isoliert werden. Im zweiten Schritt folgt die Systemsicherung. Noch vor dem Löschen und erneuten Abbilden eines Systems ist es notwendig, ein forensisches Abbild der betroffenen Systeme zu erstellen. Forensische Software erfasst die betroffenen Systeme so, wie sie während des Störfalls waren. Diese Sicherung kann später als Beweismittel genutzt werden.

Im dritten Schritt sollten die betroffenen Systeme kurzfristig und vorübergehend in einen sicheren und arbeitsfähigen Zustand gebracht werden, damit sie bei Bedarf weiter in der laufenden Produktion eingesetzt werden können. Im Vordergrund stehen hier die Entfernung von Angreifer-Accounts und -Hintertüren, das Entfernen von Schadsoftware, die Installation von Sicherheitspatches auf betroffenen und angrenzenden Systemen sowie weitere Maßnahmen, um eine weitere Eskalation des Incidents zu vermeiden und den normalen Geschäftsbetrieb fortsetzen zu können. Diese vorübergehend gepatchten und sicheren Systeme werden im nächsten Schritt durch saubere und neu aufgebaute Systeme ersetzt.

05 BEREINIGUNG

In dieser Phase werden Deinstallation und Wiederherstellung der betroffenen Systeme durchgeführt. Eine fortlaufende Dokumentation aller ergriffenen Maßnahmen ist erforderlich, um die Kosten für Arbeitsstunden und andere Ressourcen als Grundlage für die Ermittlung der Gesamtauswirkungen auf das Unternehmen zu ermitteln. Auch müssen schädliche und andere betrügerische Inhalte von den betroffenen Systemen entfernt und dann bereinigt werden. Nur durch eine vollständige Sicherung der Festplatten kann eine erneute Infektion verhindert werden. Nachdem die Ursache für den Störfall herausgefunden wurde, sollte die Abwehr verbessert werden, um eine erneute Infizierung auszuschließen.

06 WIEDER-HERSTELLUNG

Ziel dieser Phase ist die Wiederherstellung der betroffenen Systeme in die Produktionsumgebung, damit sie nicht zu einem weiteren Incident führen. Ein Test der wieder in Betrieb genommenen Systeme ist unerlässlich, ebenso die Überwachung und Validierung dieser. Dadurch wird sichergestellt, dass die Systeme nicht durch Malware reinfiziert oder auf andere Weise gefährdet werden.

Einige der am wichtigsten zu treffenden Entscheidungen in dieser Phase sind:

- Die Systembetreiber müssen eine endgültige Entscheidung über die Zeitangaben für die Wiederherstellung der Abläufe treffen.
  Sie sollten sich hier auf die Empfehlungen des CIRT verlassen.

- Müssen weitere Schutzmaßnahmen vor der erneuten Inbetriebnahme ergriffen werden? Hierzu gehört beispielsweise eine verbesserte Härtung der Betriebssysteme oder die Optimierung der Antivirensoftware durch die suresecure.

- Wie wird getestet und geprüft, ob die betroffenen Systeme fehlerfrei und voll funktionsfähig sind?

- Es sollte ein Zeitplan erstellt werden, in dem die Überwachung auf abnormales Verhalten festgelegt wird.

- Welche Tools sollen zum Testen, Überwachen und Validieren des Systemverhaltens eingesetzt werden?

- Sind wir in der Lage den Incident alleine zu beheben oder brauchen wir die Unterstützung der suresecure?

07 LESSONS LEARNED

Diese Phase ist neben der Vorbereitung die kritischste. Die Aufzeichnungen müssen vervollständigt und fehlende Informationen zusammengetragen werden. Auch Informationen, die für einen zukünftigen Incident wichtig sein könnten, gehören in diesen Bericht. Der Bericht dient der Durchführung einer detaillierten Analyse des gesamten Ereignisses und muss Antworten auf folgende Fragen bereitstellen: Wer, was, wo, warum und wie? Das übergeordnete Ziel ist, innerhalb eines Unternehmens aus den Geschehnissen zu lernen, die richtigen Schlüsse zu ziehen und den Incident Response zu optimieren.

Dadurch wird die Leistung des Teams verbessert und im Falle eines ähnlichen Vorfalls kann Referenzmaterial bereitgestellt werden. Die Dokumentation kann auch als Trainingsmaterial für neue Teammitglieder oder als Vergleichsmaterial für zukünftige Krisen verwendet werden. Das Lessons Learned Meeting sollte frühzeitig durchgeführt werden, in der Regel innerhalb von zwei Wochen nach dem Incident. In dem Meeting wird der Bericht über die Maßnahmen durchgearbeitet und in einem Leitfaden festgehalten.

Folgende Informationen sollten zusammengefasst und festgehalten werden:

- Wann wurde der Incident zum ersten Mal festgestellt?
- Wer hat den Incident festgestellt?
- Das Ausmaß des Incidents
- Die Art und Weise, wie der Incident abgefangen und beseitigt wurde
- Arbeitsergebnisse der Verarbeitung
- Bereiche, in denen das CIRT-Team erfolgreich war
- Bereiche, die optimiert werden müssen

Um die Effektivität des Teams bei zukünftigen Störfällen zu erhöhen, empfiehlt sich auch das Handeln des CIRTs zu reflektieren.

07 CHECKLISTE

IDENTIFIKATION

- Wo fand der Incident statt?
- Wer hat den Incident entdeckt und gemeldet?
- Wie wurde der Incident entdeckt?
- Welche Bereiche werden beeinträchtigt?
- Wie groß sind die Auswirkungen?
- Wie wirkt sich das auf das Unternehmen aus?
- Wurde die Quelle(n) des Incidents lokalisiert? Wo, wann, was?

KURZFRISTIGE SICHERHEITSMASSNAHMEN

- Alle zuständigen Personen alarmieren!
- Das Problem eindämmen!
- Nicht betroffene Systeme isolieren!
- Zugriffe beschränken!

SYSTEM-BACKUP

- Für forensische Zwecke Backups der betroffenen Systeme erstellen!
- Alle Maßnahmen lückenlos dokumentieren, inklusive Fotos!
- Beweise sichern!
- Die forensischen Sicherungskopien an einem sicheren Ort aufbewahren!

07 CHECKLISTE

LANGFRISTIGE SICHERHEITSMASSNAHMEN

- Systeme, die offline geschaltet werden können: löschen!
- Systeme, die online bleiben müssen: eindämmen!

BESEITIGUNG

- Das System neu abbilden und mit Gegenmaßnahmen absichern!
- Alle Malware und andere Artefakte entfernen!
- Betroffene Systeme gegen weitere Angriffe absichern!

WIEDERHERSTELLUNG

- Sicherstellen, dass alle betroffenen Systeme gepatcht wurden und gegen die aktuellen wie gegen potenzielle, zukünftige Angriffe abgesichert sind!
- Zeitpunkt festlegen, um die betroffenen Systeme wieder in Betrieb zu nehmen!
- Zeitplan erstellen, wie lange die wiederhergestellten Systeme überwacht werden sollen und wonach gesucht werden soll!
- Vorhandene Benchmarks für den Vergleich bereithalten!

07 CHECKLISTE

LESSONS LEARNED

- Kontrolle der Dokumentation! Wer? Was? Wo? Warum? Wie?
- Zeitnahen Erfahrungstausch durchführen!
- Rückblick und Analyse des Prozesses mit dem gesamten Team!

Die suresecure kontaktieren: +49 (0) 2156 9749 110!

Dennoch: Ein Incident Response macht nur einen Teil des gesamten Notfallmanagements in Unternehmen aus. Die Mitarbeiter der suresecure verfügen über langjährige, praktische Erfahrungen im Bereich des IT-Notfallmanagements. Wir helfen Ihnen gerne bei der Erstellung einer Sicherheitsstrategie für Ihr Unternehmen.

sure[secure]

VERHALTEN BEI EINEM IT-SICHERHEITSVORFALL

Ruhe bewahren & IT-Sicherheitsvorfall melden
Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallrufnummer: +49 (0) 2156 9749 110

IT-Notfallrufmail: 911@suresecure.de

- Wer sind Sie?
- Was ist passiert?
- Welche Systeme sind betroffen?
- Wann ist das passiert?
- Wo soll sich unser IT-Security Spezialisten Team einfinden?

Als Experten der IT-Security können wir auf Wunsch mit unserem Incident Response Service die Erstreaktion auf erfolgte Angriffe übernehmen und die notwendigen, ersten Schritte zum Schutz Ihrer Umgebung selbstständig einleiten.

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen	Beobachtungen dokumentieren	Maßnahmen nur nach Anweisung einleiten

suresecure GmbH
Hausbroicher Str. 296D
47877 Willich

Telefon: +49 (0) 2156 974 90 60
Telefax: +49 (0) 2156 975 49 78

E-Mail: info@suresecure.de
www.suresecure.de