SWS
COMPUTERSYSTEME
Member of ACP Group

NOTFALLPLAN

IT for innovators.
Member of ACP Group

Inhaltsverzeichnis

1 Einleitung 2

2 Erste Hilfe bei Sicherheitsvorfall für Nutzer 2

2.1 Ruhe bewahren und Hilfe holen! 2

2.2 Dokumentieren von Informationen 2

2.3 Systeme eingeschaltet lassen 2

2.4 Netzwerkverbindung trennen 3

2.5 Sichere Kommunikationswege 3

3 Erste Hilfe bei Sicherheitsvorfall für Administratoren 3

3.1 Netzwerksegmente trennen (Ransomware) 4

3.2 Kernsysteme schützen 4

3.3 Sicherung der Backups und Logs 4

4 Kommunikation und Ansprechpartner 5

1 Einleitung

Bei einem Angriff auf IT-Systeme ist eine ruhige und koordinierte Vorgehensweise sehr wertvoll, um auf den Vorfall entsprechend zu reagieren und diesen bestmöglich aufklären zu können. Die ersten Personen, die auf einen potenziellen Angriff aufmerksam werden sind oftmals die Nutzer und Mitarbeiter selbst. Dieses Dokument soll Nutzern von IT-Systemen und Administratoren helfen, einen Vorfall möglicherweise rechtzeitig zu erkennen und eine Anleitung geben, wie in einem solchen Fall vorzugehen ist.

2 Erste Hilfe bei Sicherheitsvorfall für Nutzer

2.1 Ruhe bewahren und Hilfe holen!

Während eines Sicherheitsvorfalls ist es wichtig, dass Sie Ruhe bewahren. Sollte ein begründeter Verdacht auf einen Angriff vorliegen, bleiben Sie ruhig und kontaktieren Sie schnellstmöglich Hilfe, sodass ein möglicher Schaden zeitnah eingedämmt werden kann.
Sind Sie sich nicht sicher, sollte der Vorfall dennoch gemeldet und untersucht werden, auch wenn sich der Verdacht nicht bestätigen sollte.

2.2 Dokumentieren von Informationen

Notieren Sie auffälliges Verhalten und Informationen inklusive deren Uhrzeit auf Papier oder dem Smartphone. Aktionen auf dem möglicherweise befallenen System sind zu vermeiden, da diese zum einen Beweise vernichten und zum anderen den Angreifer alarmieren könnten.

2.3 Systeme eingeschaltet lassen

Es wird empfohlen betroffene Systeme grundsätzlich eingeschaltet zu lassen. Im schlimmsten Fall wird durch ein Herunterfahren der Angreifer alarmiert, woraufhin dieser dann möglicherweise destruktive Aktionen ausführt. Zudem befinden sich wichtige Beweise im Arbeitsspeicher, die durch ein Herunterfahren vernichtet werden.

Ein Ausnahmefall besteht dann, wenn es sich um einen laufenden Ransomware Angriff handelt, bei dem Dateien verschlüsselt werden und/oder das System nicht vom Netzwerk getrennt werden kann. Besteht die Möglichkeit das System in den Ruhezustand (Hibernation) Modus zu versetzen, ist dies dem kompletten Herunterfahren vorzuziehen, da somit der Arbeitsspeicher erhalten wird.

2.4 Netzwerkverbindung trennen

Bemerkung: Solange das System noch mit dem Netzwerk verbunden ist, darf keinesfalls ein Benutzer mit Administratorrechten angemeldet werden!

Eine pauschale Aussage, ob die Netzwerkverbindung getrennt werden soll, ist schwierig zu treffen. Dies hängt nämlich von der aktuellen Situation ob und ist pro Fall individuell zu treffen. Generell lässt sich jedoch Folgendes sagen.

Wurde der Vorfall durch den Benutzer selbst initiiert, beispielsweise durch Öffnen einer bösartigen Datei, oder handelt es sich um einen laufenden Ransomware Angriff, dann ist die Netzwerkverbindung umgehend zu trennen! Dies soll eine weitere Ausbreitung im Netzwerk verhindern.
Systeme können durch Ziehen des Netzwerkkabels und durch Deaktivieren des WLAN Adapters vom Netzwerk getrennt werden. Achten Sie darauf, dass tatsächlich beide Möglichkeiten deaktiviert sind.

Ist das System vermeintlich schon länger kompromittiert oder befindet sich der Angreifer schon länger auf dem System, dann sollte die Netzwerkverbindung aufrechterhalten werden. Dies könnte ansonsten den Angreifer alarmieren.

2.5 Sichere Kommunikationswege

Während eines Sicherheitsvorfalls ist davon auszugehen, dass ein Angreifer auch die Kommunikation überwacht, um sensitive Informationen zu erlangen. Dazu gehören unter anderem auch Mailserver oder Telefondienste. Soweit möglich sollte die Kommunikation auf sicherem Weg, etwa über private Handys oder direkte Treffen erfolgen.

3 Erste Hilfe bei Sicherheitsvorfall für Administratoren

Zusätzlich zu den obigen Punkten können Administratoren oft zusätzliche Schritte ausführen, die einen Sicherheitsvorfall eindämmen können und zur Aufklärung beitragen.

3.1 Netzwerksegmente trennen (Ransomware)

Sind bei einem laufenden Ransomwarevorfalls bereits mehrere Systeme betroffen oder wird eine weitere Ausbreitung vermutet, dann reicht es nicht aus, die Systeme einzeln zu trennen. An dieser Stelle trennen Sie das Netzwerksegment vom restlichen Netzwerk, um eine weitere Ausbreitung zu verhindern.

Ist ein Trennen auf Netzwerksegmentebene nicht möglich, sind folgende Möglichkeiten in Betracht zu ziehen, um eine weitere Ausbreitung zu verhindern:

- Abschalten Router/Switch
- Verbindung zwischen Standorten/Netzwerken trennen
- Internetverbindung des Standorts trennen
- Noch nicht befallene Systeme vom Netzwerk trennen

3.2 Kernsysteme schützen

Die Kernsysteme, die geschäftskritisch sind, sollten im Falle einer ausbreitenden Infektion geschützt bzw. isoliert werden, damit deren Betrieb oder deren Daten sichergestellt sind.

3.3 Sicherung der Backups und Logs

Besitzen Sie Datensicherungen der Systeme, dann ist diese zu schützen. Dies ist möglicherweise die einzige Möglichkeit verlorene Daten wiederherzustellen und Systeme ohne Datenverlust zu bereinigen. Sorgen Sie dafür, dass bestehende Backups nicht überschrieben werden, etwa durch Rotation der Backups, oder der Angreifer diese manipulieren bzw. löschen kann.

Ähnliches gilt für Logdaten. Bereits gesammelte Logs sind zu sichern (z.B. Firewall, Proxy, Windows Security Log, ..) und vor Manipulation und vor dem Überschreiben zu schützen.

Zudem sollte das Protokollierungslevel auf den Systemen im Netzwerk erhöht werden, sodass möglichst viele Informationen über den Vorfall gesammelt werden können und dieser bestmöglich aufgeklärt werden kann. An dieser Stelle ist es notwendig den Datenschutzbeauftragten über das Sammeln dieser Informationen zu benachrichtigen.

4 Kommunikation und Ansprechpartner

Versuchen Sie den Personenkreis, der über den Vorfall Bescheid weiß, möglichst klein zu halten. Initial ist oftmals nicht klar, ob der Angriff von einem externen oder internen Angreifer ausgeht. Im Beispiel eines Datendiebstahls durch einen eigenen Mitarbeiter sollte dieser möglichst nichts erfahren, damit möglichst viele Beweise gesammelt werden können.

Nachfolgend sind die Kontaktdaten von möglichen Ansprechpartnern:

Verantwortlicher Abteilungsleiter der IT oder Chief Information Officer („CIO“) des Unternehmens

- Bestellter Datenschutzbeauftragter der Organisation
- Unternehmensführung in Form des Geschäftsführers oder Vorstandes
- Vorsitzender des Aufsichtsrates• Rechtsabteilung oder externe Rechtsanwaltskanzlei
- Betriebsrat, Personalrat oder entsprechende Mitarbeitervertretung
- Pressesprecher oder externe PR Agentur

Die Spezialisten der Polizei

Die Unternehmensleitung sollte spätestens jetzt entscheiden, ob Strafverfolgungsbehörden eingeschaltet werden sollen.

1. Bundeskriminalamt: +49 611 55-15037 E-Mail: zac@cyber.bka.de
2. Bayern: +49 89 1212-3300 E-Mail: zac@polizei.bayern.de
3. NRW: +49 211 939-4040 E-Mail: cybercrime.lka@polizei.nrw.de
4. Baden-Württemberg: +49 711 5401-2444 E-Mail: cybercrime(at)polizei.bwl.de
5. Europol EC3: +31 70 302 5000
6. https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html