r tec
cyber security

WHITEPAPER

Incident-Response-Readiness-Checkliste

Incident Response Readiness: Vorbereitung auf den Angriffsfall

In Anbetracht der Geschwindigkeit, mit der sich Angreifer heutzutage in gekaperten Netzwerken ausbreiten können, ist eine gute Vorbereitung der wichtigste Baustein, um Reputationsverluste und finanzielle Schäden vom eigenen Unternehmen abzuwenden. In diesem Whitepaper erfahren Sie, welche Vorbereitungen getroffen werden müssen, um im Falle eines Security Incidents schnell und geplant reagieren zu können.

Zunächst verdeutlichen wir anhand eines beispielhaften Angriffshergangs das Vorgehen sowie die Geschwindigkeit eines typischen Angreifers und zeigen die Ausmaße einer solchen Attacke auf. Anschließend betrachten wir den Standard-Incident-Response-Prozess, den das r-tec Incident Response Team täglich in der Praxis einsetzt. Durch einen genauen Blick auf unser Vorgehen wird deutlich, welche Maßnahmen im Rahmen der Incident-Behandlung durch eine gute Vorbereitung beschleunigt oder überhaupt erst möglich gemacht werden. Auf Basis der daraus resultierenden Erkenntnisse leiten wir letztlich eine Checkliste mit technischen sowie nichttechnischen Maßnahmen ab, die umgesetzt werden sollten, um auf einen Security Incident vorbereitet zu sein und im Falle eines Angriffs die erforderliche Geschwindigkeit an den Tag legen zu können.

Praxisbeispiel: Vom initialen Zugriff zur Systemverschlüsselung in fünf Tagen

Die folgende Abbildung skizziert die Tätigkeiten eines Angreifers, die r-tec im Rahmen eines Incident-Response-Einsatzes rekonstruieren konnte. Nennenswert ist vor allem die Geschwindigkeit, mit der sich der Angreifer im Unternehmensnetzwerk ausbreiten und Schaden anrichten konnte. Komponenten, die dafür benötigt werden, skizziert das vorliegende Whitepaper.

Incident Response

Tag 0 (Montag)
- Erstinfektion eines Benutzers über Phishing
- Zugriff über erbeutete Zugangsdaten

Tag 1 (Dienstag)
- Privilege Escalation: Lokaler Admin auf Domainadministrator

Tag 2 (Mittwoch)
- Lateral Movement: Cobaltstrike Loader auf weitere Systeme verteilt

Tag 3 (Donnerstag)
- Einrichtung Datenplattform auf Backup-Server

Tag 4 (Freitag)
- Aktive Remote Desktop Session

Tag 5 (Samstag)
- Verschlüsselung von Systemen
- Erpresserschreiben

Tag 0_ Die ersten Aktivitäten lassen sich in die Beschaffung von Zugangsdaten und den initialen Zugriff auf Ressourcen des Zielunternehmens unterteilen. Häufig findet die Entwendung von Zugangsinformationen nicht mehr durch den späteren Angreifer statt, sondern durch sogenannte Network Access Broker. Diese sind spezialisiert darauf, Zugangsinformationen von Unternehmen zu sammeln und diese über das Darknet an die späteren eigentlichen Angreifer zu verkaufen.

Tag 1_ Mithilfe der bekannten Zugangsinformationen versucht der Angreifer, seine Rechte zu erhöhen. Ziel ist es, zunächst lokale Administratorrechte und schließlich Domainadministratorrechte zu erhalten.

Tag 2_ Im nächsten Schritt versucht der Angreifer, seinen Zugriff auf das Netzwerk des Zielunternehmens mittels bekannter Werkzeuge – in diesem Beispiel Cobalt Strike – auszuweiten. Kontrolliert werden die übernommenen Clients mithilfe eines C2-Servers (Command and Control), zu dem eine Verbindung aufgebaut wird.

Tag 3_ Um Daten aus dem Zielunternehmen zu extrahieren, benötigt der Angreifer eine Datenplattform, auf der Informationen zunächst im Unternehmensnetz gesammelt und dann aus dem Unternehmen abgeführt werden können. Häufig werden hierfür Backup-Server verwendet. Backup-Server fallen aufgrund ihrer Funktion nicht weiter auf, wenn vermehrt Verbindungen aufgebaut und Daten übertragen werden.

Tag 4_ Der Angreifer meldet sich auf unterschiedlichen Systemen an und sammelt Informationen.

Tag 5_ Nachdem der Angreifer genug Informationen gesammelt und aus dem Unternehmen herausgeschleust hat, folgt die Verschlüsselung von Systemen und ein Erpresserschreiben mit der Aufforderung, Bitcoin zu transferieren.

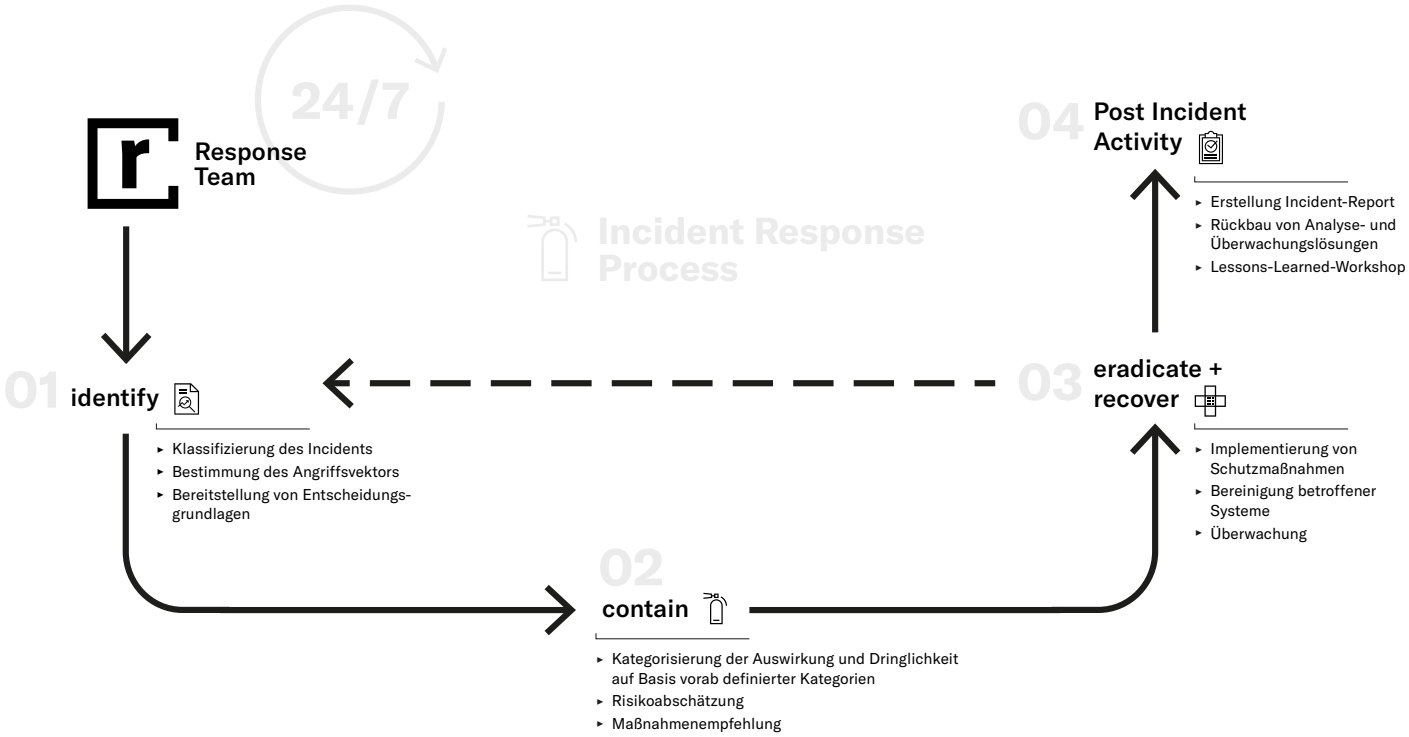
Schadensbilanz_ Der hier skizzierte Angriff fand über ein verlängertes Wochenende statt, und hat 10 Mitarbeiter des Zielunternehmens über eine Woche (inkl. Wochenende und Überstunden) gebunden. Zusätzlich waren externe Analysten und Engineers über 100 Stunden mit der Bearbeitung des Vorfalls beschäftigt. Aufgrund der frühen Erkennung und dem Umstand, dass in diesem Fall keine Daten entwendet wurden, ist die Schadenssumme verhältnismäßig niedrig und wird auf insgesamt 100.000 € geschätzt.

Insbesondere in Anbetracht der Geschwindigkeit, mit der sich Angreifer nach dem initialen Zugriff im Unternehmen ausbreiten und Informationen abgreifen können, ist das schnelle und planvolle Vorgehen das beste Mittel, um Schaden zu minimieren.

Incident Response

Die vier Phasen des Incident-Response-Prozesses

Um einen Überblick darüber zu erhalten, was für eine gute Vorbereitung erforderlich ist, hilft ein Blick auf das Standardvorgehen, das das r-tec Incident Response Team täglich bei der Behandlung von Security Incidents einsetzt. Das Vorgehen kann in vier Phasen unterteilt werden, die gegebenenfalls mehrfach durchlaufen werden müssen.



01. Identifizierung

- Klassifizierung des Incidents nach bewährter Taxonomie
- Analyse von Dateien, Systemen, E-Mails, Logfiles, Netzwerkverkehr etc.
- Anfertigen von Datenträger- und Speicherabbildern
- Bestimmung des individuellen Angriffsvektors
- Ermittlung des Ausmaßes, insbesondere in Bezug auf betroffene Bereiche und den zeitlichen Ablauf
- Erstellung forensischer Analysen
- Einschätzung der Gefährdungslage
- Bereitstellung von Entscheidungsgrundlagen

02. Eindämmung

- Entwicklung von Sofortmaßnahmen
- Vermeidung der Ausbreitung eines Vorfalls
- Abwehr von aktiven Angriffen

03. Bereinigung und Wiederherstellung

- Implementierung von Schutzmaßnahmen gegen Neuinfizierung
- Bereinigung betroffener Assets mithilfe der ermittelten Informationen
- Wiederherstellung von einzelnen Assets
- Koordinierte Änderung von kompromittierten Zugriffen und Zugangsdaten
- Koordinierte Wiederherstellung des Regelbetriebs
- Überwachung der erfolgreichen Bereinigung

04. Nachbereitung

- Erstellung eines Incident-Reports
- Rückbau temporärer Analyse- und Überwachungslösungen
- Lessons-Learned-Workshop zur Optimierung der Incident-Response-Fähigkeiten im Rahmen des kontinuierlichen Verbesserungsprozesses

Anhand der einzelnen Phasen lassen sich die Vorbereitungsmaßnahmen in zwei Kategorien einordnen: technische und nichttechnische Maßnahmen.

Die nachfolgende Checkliste ist als ein Leitfaden zu verstehen und keinesfalls abschließend. Zahlreiche Kriterien wie die Unternehmensgröße oder die Branche, in der ein Unternehmen tätig ist, haben einen Einfluss darauf, welche Maßnahmen zur Vorbereitung sinnvoll sind.

Checkliste

Nichttechnische Maßnahmen

BEREICH	MAßNAHME	
Organisation	Wurden Rollen und Verantwortlichkeiten definiert?	☐
	Ist sichergestellt, dass im Notfall schnelle Entscheidungen getroffen werden können (z. B. durch Abschalten von geschäftskritischen Systemen oder Freigabe von Budgets)?	☐
Prozess	Existiert ein Incident-Response-Prozess, der dokumentiert und allen betroffenen Personen bekannt ist?	☐
	Wurden Meldewege für Incidents definiert und im Unternehmen bekannt gegeben?	☐
	Existiert eine einheitliche Vorgehensweise für die Klassifizierung und Priorisierung von Incidents?	☐
	Wurden Reaktionszeiten für Incidents definiert?	☐
	Wurden Eskalationswege definiert?	☐
	Sind alle externen Meldepflichten in Bezug auf einen Sicherheitsvorfall bekannt und dokumentiert?	☐
	Sind alle internen Meldepflichten in Bezug auf einen Sicherheitsvorfall bekannt und dokumentiert?	☐
	Wurden alternative Kommunikationskanäle definiert?	☐
	Existieren Kontaktlisten für wichtige Parteien bei einem Incident (z. B. interne Kontakte, Dienstleister, Behörden)?	☐
	Ist geklärt, wie im Notfall eine Analyse von Logdaten oder Systemen durchgeführt werden kann (z. B. durch eine Generalvereinbarung mit dem Betriebsrat)?	☐
Personen	Ist qualifiziertes Personal für die Behandlung von Incidents in ausreichender Menge vorhanden (insbesondere um Reaktionszeiten nachts, am Wochenende oder an Feiertagen zu gewährleisten)?	☐
	Ist gewährleistet, dass das Personal im Notfall von seinen Aufgaben im Tagesgeschäft freigestellt werden kann?	☐
Pläne und Vorlagen	Existieren Ablaufpläne (Playbooks) für einzelne Vorfallstypen (z. B. Ransomware)?	☐
	Existiert ein Dokument, das den Incident-Response-Prozess beschreibt und dokumentiert (Incident-Response-Plan)?	☐
	Existieren Vorgaben oder Vorlagen für die Dokumentation von Incidents?	☐
	Sind die Dokumente/Vorgaben/Richtlinien auch offline verfügbar und von mehreren Mitarbeitern zu erreichen?	☐
	Existieren Vorgaben für die Archivierung von Informationen zu abgeschlossenen Incidents?	☐

Checkliste

Kontinuierliche Verbesserung	Existiert eine Knowledge Base für Incidents?	☐
	Werden Pläne, Vorlagen und andere begleitende Dokumente auf erforderliche Aktualisierungen überprüft?	☐
	Werden Kennzahlen zu Incidents erhoben (z. B. Kategorie, Klassifizierung)?	☐
	Wird das eingesetzte Incident Response Team regelmäßig geschult?	☐
	Werden Planspiele für ausgewählte Angriffstypen durchgeführt?	☐
	Werden unangekündigte Angriffssimulationen durchgeführt (Red Teaming)?	☐
	Werden die technischen Response-Fähigkeiten einer Überprüfung unterzogen?	☐

Technische Maßnahmen

BEREICH	MAßNAHME	
Event Logging	Benötigt wird ein zentrales Log-, Monitoring- und Reporting-Tool, in das folgende Produkte bzw. Dienste Logdateien einliefern:	
	▸ Firewall (Perimeter etc.)	☐
	▸ Intrusion-Prevention- und Intrusion-Detection-System	☐
	▸ Network Access Control	☐
	▸ Web und Mail-Flow	☐
	▸ Client und Server Logging	☐
	▸ Remote Access / VPN / VDI (z. B. Netscaler)	☐
	▸ Cloud-Services	☐
Identifizierung	Existiert ein Asset-Inventar?	☐
	Sind Tools und Technologien für forensische Analysen vorhanden?	☐
	Existieren Netzwerkpläne?	☐
	Existiert ein Fernzugriff auf das Unternehmensnetzwerk?	☐
	Existiert eine zentrale Softwareverteilung?	☐
Eindämmung	Existieren Systeme zur Erkennung von Malware?	☐
	Existieren Möglichkeiten, Endgeräte zu isolieren?	☐
	Ist der Support von Betriebssystemen, Plattformen etc. durch den Hersteller sichergestellt?	☐
	Ist ein Intrusion-Prevention-System im Einsatz?	☐
Bereinigung und Wiederherstellung	Ist sichergestellt, dass Backups zurückgespielt werden können?	☐
	Existieren Möglichkeiten, eine als sicher bekannte Konfiguration auf Systeme auszurollen?	☐
	Existieren Lösungen zur Systemhärtung?	☐

Die r-tec IT Security GmbH mit Sitz in Wuppertal wurde 1996 von Dr. Stefan Rummenhöller gegründet. Als Wegbereiter und Wegbegleiter schaffen wir für unsere Kunden sichere Räume für die Entwicklung ihrer Organisationen und die Verwirklichung ihrer Visionen. Unsere Kunden aus dem gehobenen Mittelstand, Konzerne, kommunale Rechenzentren und Bundes- oder Landesbehörden vertrauen seit über 20 Jahren auf unsere hoch spezialisierten Experten.

Als Strategic Supplier für Cyber Security Services schützen wir die Werte unserer Kunden vor Bedrohungen und begleiten ihr Security Management von der Initiierung über die Einführung bis zum Betrieb auf allen Ebenen.

Wir leben Regeltreue, höchste Qualitätsstandards und Servicementalität. Unser Unternehmen haben wir nach den Strukturen und Richtlinien der DIN ISO 9001:2015 und der ITIL aufgebaut. Wir sind nach ISO 27001 zertifiziert.

r-tec IT Security GmbH | Hatzfelder Str. 165–167 | 42281 Wuppertal
www.r-tec.net | +49 (0) 202 31767–100