

Prep for Response!

Notwendige Vorbereitungen für die Vorfallsbehandlung

Wie so oft in der Security gilt auch beim Incident-Response: Wer erst im Falle eines Falles plant, hat schon verloren. Für die Behandlung von IT-Sicherheitsvorfällen sind eine Menge Dinge vorab zu klären, zu veranlassen, zu schulen und nicht zuletzt auch zu üben. Dabei können einschlägige Normen, Playbooks und Checklisten gute Hilfestellung leisten.

Von *Joshua Tiago, Heilbronn*

Angesichts der IT-Durchdringung fast aller Bereiche von Wirtschaft und Gesellschaft können selbst vermeintlich kleine Sicherheitslücken heute ohne eine strukturierte Incident-Response-Strategie und eine gründliche Vorbereitung schwerwiegende Folgen haben: Datenverlust, Betriebsunterbrechungen, finanzielle Schäden und Reputationsverlust sind häufige Ergebnisse eines erfolgreichen Angriffs.

Ein schnelles, koordiniertes Vorgehen ist entscheidend, um die Auswirkungen von Angriffen zu begrenzen. Studien zeigen, dass Unternehmen mit einem etablierten IR-Prozess Sicherheitsvorfälle deutlich schneller erkennen und eindämmen können. Das spart nicht nur Kosten, sondern schützt auch vor rechtlichen Konsequenzen (etwa durch die DSGVO) und einem Vertrauensverlust bei Kunden. Zudem verlangen viele Compliance-Richtlinien (z. B. ISO 27001 oder KRITIS) explizit nachweisbare Incident-Response-Pläne.

Technische Maßnahmen allein genügen jedoch nicht: Ohne klar definierte Prozesse, geschultes Personal und regelmäßige Übungen drohen im Ernstfall Unsicherheit, unüberlegtes Handeln und Verzögerungen. Eine gute Vorbereitung stellt sicher, dass alle Beteiligten wissen, was im Notfall zu tun ist, und dass das Unternehmen auch nach einem Angriff handlungsfähig bleibt. Incident Response ist keine Option, sondern eine Notwendigkeit für jede Organisation, die langfristig resilient bleiben will.

Die organisatorische Seite

Für eine schnelle und effektive Reaktion auf einen Vorfall spielt die organisatorische Seite eine entscheidende Rolle. Verantwortliche in Unternehmen neigen häufig dazu, primär technische Maßnahmen zu betrachten – gerade wenn Unternehmen zum ersten Mal über Incident-Response (IR) nachdenken, scheinen techni-

sche Maßnahmen und Werkzeuge die naheliegendsten Antworten auf einen Sicherheitsvorfall zu geben. In der Praxis zeigt sich aber sehr schnell, dass dies allein nicht ausreicht: Ohne ein abgestimmtes organisatorisches Vorgehen ist eine effiziente Behandlung eines Vorfalls nur bedingt durchführbar.

Das Problem in Unternehmen ohne ausgereifte IR-Strategie beginnt häufig bereits beim Thema „Rollen und Zuständigkeiten“ – hier stellen sich folgende Fragen:

- _____ Wer meldet wann, wem und wie einen Vorfall?
- _____ Wer ist verantwortlich für die Bearbeitung eines Vorfalls?
- _____ Wer entscheidet, ob es sich überhaupt um einen Vorfall handelt?
- _____ Wer entscheidet, ob ein kritisches System abgeschaltet werden muss?
- _____ Wer entscheidet, ob Kunden, Geschäftspartner, die Behörden oder die Öffentlichkeit über den Vorfall unterrichtet werden müssen?
- _____ Wer entscheidet, ob und wann externe Experten zur Bewältigung des Vorfalls hinzugezogen werden sollen?

Diese Fragen zeigen deutlich, dass es zu Beginn der Reaktion auf Vorfälle nicht darum geht, welche technischen Maßnahmen man treffen soll oder welche Werkzeuge zum Einsatz kommen. In einem Umfeld, in dem die aufgeführten Fragen nicht im Vorfeld geklärt wurden, sind alle Beteiligten verunsichert – Entscheidungen müssen ad hoc getroffen werden. Unsicherheit, Angst und Ungewissheit sind in solchen Situationen allerdings ein schlechter Ratgeber. Hinzu kommt Verunsicherung bei den Mitarbeitern darüber, ob sie ihre Kompetenzen überschreiten: Fehlentscheidungen zu diesem Zeitpunkt können jedoch gravierende Folgen haben. Der Vorfall wird möglicherweise falsch bewertet, notwendige Schritte werden nicht eingeleitet oder gesetzliche Vorgaben nicht eingehalten.

Die genannten Fragen betreffen dennoch nur einen kleinen Teil der Themen, die im Sinne einer organisatorischen Vorbereitung geklärt werden müssen. Wie sieht also eine gute Vorbereitung auf der organisatorischen Seite für Unternehmen aus? Unternehmen sind sehr unterschiedlich aufgestellt. Die Anforderungen an ein regionales Unternehmen mit 100 Mitarbeitern* unterscheiden sich stark von denen eines international operierenden Konzerns mit 100 000 Mitarbeitern.

Normative Grundlagen

Eine IR-Strategie oder einen IR-Plan, die sich für alle Unternehmen gleichermaßen anwenden ließen, kann es also gar nicht geben. Stattdessen orientieren sich Unternehmen in vielen Fällen an internationalen Normen oder Frameworks für die Etablierung eines IR-Plans und einer übergeordneten IR-Strategie. In der Praxis haben sich die ISO 27035 „Information technology — Information security incident management“ [1] sowie die NIST SP 800-61 „Computer Security Incident Handling“ [2] bewährt (die aktuelle Fassung der NIST SP 800-61 ist im April als „Incident Response Recommendations and Considerations for Cybersecurity Risk Management“ [3] erschienen).

Beide Normen dienen als Rahmenwerk, um Incident-Response sowohl in kleinen als auch in großen Unternehmen strukturiert aufzubauen. Die Normen sind jedoch nicht als Schritt-für-Schritt-Anleitung zu verstehen – stattdessen werden die notwendigen Aspekte rund um das Thema Incident-Response beschrieben und an manchen Stellen durch konkrete Handlungsempfehlungen ergänzt. Die Aufgabe für Unternehmen besteht also darin, eine IR-Strategie oder IR-Prozesse an den genannten Normen auszurichten.

Es kann kaum überraschen, dass das Thema „Rollen und Zuständigkeiten“ dabei besonders relevant ist: Wie in ISO 27035 beschrieben, können die im Rahmen eines Vorfalls häufig anfallenden Aufgaben nicht allein von Kollegen aus den unterschiedlichen IT-Bereichen übernommen werden. Vielmehr ist von der Etablierung eines *Incident-Response-(IR)-Teams* die Rede, dessen Mitglieder verschiedene Rollen übernehmen.

Wenn wir uns die oben aufgeführten Fragen, die organisatorisch zu klären sind, in Erinnerung rufen, dann ist offensichtlich, dass es sich in manchen Fällen nicht um reine IT-Themen und -Verantwortlichkeiten handelt. Aus diesem Grund empfehlen die Normen, bei der Etablierung eines IR-Teams Kollegen aus den folgenden Bereichen zu berücksichtigen:

- _____ IT – sowohl IT-Sicherheitsexperten, als auch System- und Netzwerkadministratoren
- _____ Human Resources (HR) / Personalabteilung

- _____ Rechtsabteilung
- _____ Öffentlichkeitsarbeit / Kommunikation

In der Praxis werden allerdings nicht alle Kollegen aus dem IR-Team an der Bearbeitung eines Vorfalls beteiligt sein. Die Unterstützung der Personalabteilung oder der Rechtsabteilung wird wahrscheinlich in den meisten Fällen nicht benötigt – in manch anderen Fällen ist deren Unterstützung aber umso wichtiger.

Der ausschlaggebende Punkt an dieser Stelle ist, dass die Mitglieder des IR-Teams nicht nur fachliche Experten in ihren Bereichen sind, sondern die notwendigen Befugnisse erhalten, um in ihrem Verantwortungsbereich jederzeit Entscheidungen treffen zu können! Es nützt nur wenig, wenn die Mitglieder im Team wissen, was zu tun wäre, sie aber keine Befugnisse haben, um zum Beispiel nachts oder am Wochenende eine schnelle Entscheidung zu treffen. Ebenfalls ist bei der Etablierung des Teams an eine Vertreterregelung zu denken – das IR-Team sollte auch während der Urlaubssaison und sonstigen Fehlzeiten einsatzfähig bleiben.

Neben den Querschnittsbereichen, aus denen das IR-Team bestehen sollte, werden in der ISO 27035 auch konkrete Rollen innerhalb des IR-Teams benannt: Allem voran sind hierbei die Rollen des Incident-Managers und der Analysten hervorzuheben:

_____ Der *Incident-Manager* ist dafür verantwortlich, im übertragenen Sinne „alle Fäden zusammenzuhalten“ und dafür zu sorgen, dass die Aufgabenverteilung sowie die Kommunikation im IR-Team und in Richtung Geschäftsführung sichergestellt sind.

_____ *Analysten* liefern hingegen wertvolle Informationen zu ausgewerteten Daten oder anderen Artefakten, die häufig als Basis für eine erste Bewertung des Vorfalls dienen. Hieraus leiten sich die konkret umzusetzenden Schritte ab: Wenn etwa eine erste Analyse ergibt, dass das Benutzerkonto eines Mitarbeiters kompromittiert wurde, müssen in der Folge diejenigen Maßnahmen in die Wege geleitet, die im Vorfeld, zum Beispiel in einem IR-Playbook zum Thema Account-Kompromittierung, definiert wurden.

Information und Austausch

Ein weiterer wichtiger Punkt auf organisatorischer Seite betrifft die Kommunikation während eines Vorfalls – und zwar sowohl extern als auch intern. Beispiele aus der Vergangenheit zeigen deutliche Unterschiede in der Kommunikationsstrategie betroffener Unternehmen: Während manche Unternehmen proaktiv, offen und rasch über Vorfälle informieren, lassen andere betroffene Kunden und die Öffentlichkeit lange Zeit in Ungewissheit. Der durch

den Vorfall möglicherweise bereits entstandene Vertrauensverlust wird dadurch nur noch weiter verschlimmert. Zu einer guten Vorbereitung gehört deshalb eine klare Regelung darüber, wer, wann, was und wie kommuniziert. Die Meldewege müssen bereits vor dem Vorfall jeder der beteiligten Personen bekannt sein. In manchen Fällen ist es ratsam, externe Unternehmen zurate zu ziehen, die sich auf Krisenkommunikation spezialisiert haben.

Bei allem Augenmerk auf externe Kommunikation sollte man nicht vernachlässigen, dass die interne Kommunikation ebenfalls eine wichtige Rolle spielt: Im Falle eines erfolgreichen Ransomware-Angriffs sind möglicherweise sehr viele Mitarbeiter direkt oder indirekt betroffen. Unter Umständen sind einige Mitarbeiter in der Folge für eine gewisse Zeit nicht mehr arbeitsfähig. Gerüchte machen in solchen Fällen schnell die Runde – manche Mitarbeiter sind vielleicht besorgt über den Fortbestand ihres Arbeitsplatzes. Eine klare und offene Kommunikation sollte die Belegschaft regelmäßig über den aktuellen Stand informieren.

Ein Punkt, der gern vergessen wird, ist überdies die Bereitstellung alternativer Kommunikationskanäle für den Fall, dass die gewohnten Wege nicht mehr zur Verfügung stehen. Gerade für Ransomware-Attacken ist es ratsam, eine Strategie zu entwerfen, um im Notfall weiterhin extern und intern kommunizieren zu können, wenn die eigene Infrastruktur nicht mehr verfügbar ist.

Vorbereitung konkreter Schritte

Die Etablierung eines IR-Teams, das Erteilen von Befugnissen und eine Strategie für die Kommunikation im Falle eines Vorfalls sind wichtige Bausteine in der Vorbereitung auf organisatorischer Ebene. Dennoch ist das erst der Anfang: Denn die Beteiligten im IR-Team sollten jederzeit wissen, was von ihnen erwartet wird und wie die konkreten Schritte aussehen.

Direkt zu Beginn eines vermeintlichen Vorfalls muss schnell bewertet werden, ob es sich um einen Fehlalarm handelt oder ob es tatsächlich Anzeichen für einen Sicherheitsvorfall gibt. Mitarbeiter, die solche Meldungen entgegennehmen, benötigen konkrete Hinweise und Anleitungen, um eine erste Bewertung vorzunehmen. Zu diesem Zeitpunkt muss rasch gehandelt werden, um gegebenenfalls mit der eigentlichen Bearbeitung des Vorfalls so schnell wie möglich zu beginnen. Checklisten oder

ein Fragenkatalog können Mitarbeiter bei der Bewertung unterstützen.

Die technische Seite

Wenn man die organisatorischen Punkte vollständig umgesetzt hat, können technische Maßnahmen zur Behandlung eines Vorfalls Hand in Hand greifen. Wie bei der Organisation sollten auch alle technischen Maßnahmen im Vorfeld geklärt, eingeführt und erprobt worden sein. Ein Sicherheitsvorfall ist der falsche Zeitpunkt, um darüber nachzudenken, welche technischen Voraussetzungen erfüllt werden müssen, um Artefakte einzusammeln, Systeme zu isolieren oder weitere IR-Maßnahmen umzusetzen.

IT-Umgebungen können je nach Unternehmen sehr groß und komplex sein – in der Vorbereitungsphase ist es daher sinnvoll, sich zu Beginn auf die wesentlichsten Systeme, Anwendungen, Daten und Geschäftsprozesse zu fokussieren. Für all diese kritischen Assets sollten Maßnahmen zur Erkennung von Sicherheitsvorfällen, zur Eindämmung und zur Analyse und Nachvollziehbarkeit eingeführt werden. Wenn es zu einem Vorfall kommt, lassen sich Daten, die man für eine erfolgreiche forensische Analyse benötigt, nicht nachträglich erheben.

Auch technische Maßnahmen zur Isolierung von Endgeräten oder ganzen Netzen können während eines Vorfalls, sofern im Vorfeld nicht bereits umgesetzt, nur sehr aufwendig und langsam eingeführt werden.

Zu einer guten Vorbereitung gehört darüber hinaus auch, die vorhandenen Vorkehrungen im Detail zu prüfen. Ein genauer Blick könnte dann zum Beispiel zutage fördern, dass zwar wichtige Ereignisse protokolliert werden, diese Informationen aber vielleicht nur eine Woche zurückreichen, was oft viel zu wenig ist. Oder es stellt sich heraus, dass die Detailtiefe der Logs nicht ausreicht oder Protokolldaten in einem proprietären Format vorliegen, was die automatisierte Auswertung enorm behindern kann.

Die Praxis zeigt, dass es häufig an Kleinigkeiten scheitert, die im Vorfeld nicht berücksichtigt wurden. Dabei geht es zum Beispiel um fehlende Freigaben oder Berechtigungen für bestimmte Systeme, unzureichende Dokumentation zu spezifischen Anwendungen oder Systemen oder schlichtweg fehlende Ressourcen, um große



Abbildung 1:
Phasen eines
Sicherheitsvorfalls
im IR-Playbook

Dateimengen während eines Vorfalls zu duplizieren und zu speichern.

Know-how und Schulungen

In der Regel kommen bei einem Vorfall neben bereits verwendeten Werkzeugen wie einer Extended-Detection-and-Response-(EDR)-Lösung weitere Werkzeuge für IR und Forensik zum Einsatz. Diese Tools sollten den Mitgliedern des IR-Teams ebenfalls im Rahmen der Vorbereitung zur Verfügung gestellt werden. Die Werkzeuge sind auf jedem Fall zu testen, um sicherzustellen, dass im Ernstfall alles wie geplant funktioniert. Das setzt wiederum voraus, dass die Mitglieder im IR-Team geschult sind, um bei Bedarf die konkreten technischen Maßnahmen umzusetzen und Analysen durchzuführen.

Viele Organisationen greifen für die Analyse und für die weitere Unterstützung während eines Vorfalls auf Dienstleister zurück, die sich auf Incident-Response spezialisiert haben. Welcher Teil dann selbst durchgeführt wird und welchen Teil der externe Incident-Responder übernimmt, variiert von Unternehmen zu Unternehmen. Dieses Vorgehen hängt üblicherweise mit den zur Verfügung stehenden Ressourcen, der Expertise eigener Mitarbeiter und anderen Faktoren zusammen. So oder so: Die Sicherstellung der relevanten Daten und Informationen bleibt in all diesen Fällen in der Regel im Verantwortungsbereich des betroffenen Unternehmens und damit des IR-Teams. Daher bleibt es auch bei Hinzuziehung eines Dienstleisters entscheidend, dass die Mitglieder im IR-Team wissen und verstehen, welche Artefakte schnell und sachgemäß gesichert werden müssen. Dabei spielen neben den technischen Herausforderungen auch Aspekte wie das Erstellen gerichtsformer Abbilder eine wichtige Rolle. Hierfür sollten die Mitglieder im IR-Team, sofern nicht bereits geschehen, geschult werden.

Trotz aller Schulungsmaßnahmen: Die meiste Erfahrung wird durch das aktive Bearbeiten von Vorfällen erlangt. Glücklicherweise muss ein IR-Team meist nicht täglich Vorfälle bearbeiten. Das führt aber auch dazu, dass die Team-Mitglieder kaum Gelegenheit haben, um die Handgriffe des Incident-Response zu üben und zu verbessern. Aus diesem Grund sollte man Vorfälle regelmäßig simulieren und üben: Ein Plan mag auf Papier detailliert und durchdacht wirken, die Realität offenbart jedoch häufig Dinge, die nicht bedacht worden sind. Solche Lücken sollten nach Möglichkeit im Rahmen einer Übung auffallen – und nicht erst bei der Bearbeitung eines realen Vorfalls.

Durch das regelmäßige Üben lässt sich gewährleisten, dass jedes Mitglied im IR-Team versteht, was und wie es zu tun ist – und dass alle Handgriffe sitzen. Auf-

wendige Szenarien zu üben, ist im Alltag allerdings oft ein Thema, das aufgrund von fehlender Zeit und Ressourcen gern in die Zukunft verschoben wird. Abhilfe schaffen können hierbei sogenannte IR-Playbooks.

IR-Playbooks

Ein IR-Playbook ist ein strukturierter Leitfaden für festgelegte Vorfallsarten. Hiermit bekommen die IR-Team-Mitglieder eine Handreichung gestellt, um im Ernstfall zu wissen, was sie tun sollen, wie sie es tun sollen und wann konkret welche Schritte anwendbar sind. Dadurch kann sichergestellt werden, dass kein Punkt während der Bearbeitung vergessen wurde. Die Bearbeitung der Vorfälle erfolgt somit strukturiert in gleichbleibender Qualität, unabhängig davon, wer im IR-Team den Vorfall bearbeitet. Dem IR-Team gibt das viel Sicherheit, da jedes Mitglied weiß, was von ihm erwartet wird und was zu tun ist.

In der Praxis bedeutet das, dass die Team-Mitglieder bei einem Vorfall das passende IR-Playbook aus der Schublade ziehen können, das ihnen die nächsten Handlungsschritte vorgibt. Ein Playbook für jeden erdenklichen Vorfall zur Verfügung zu haben, ist allerdings illusorisch: Der Aufwand für Erstellen, Erproben und Aktualisieren von IR-Playbooks ist nicht zu verachten – daher empfiehlt es sich gerade zu Beginn, die Anzahl der IR-Playbooks zu beschränken. Hierbei sollten primär Vorfallsarten berücksichtigt werden, die in der Vergangenheit bereits vorkamen, die zu erwarten sind und für die es aktuell schon Maßnahmen zur Erkennung gibt. In den meisten Fällen geht es dabei um Szenarien von Account-Kompromittierung, Phishing, Malware auf einem oder mehreren Systemen bis zu komplexen Szenarien wie Ransomware. Jedes IR-Playbook sollte die typischen Phasen eines Sicherheitsvorfalls berücksichtigen (Abb. 1).

Die jeweiligen Abschnitte in einem IR-Playbook müssen klare und konkrete Anweisungen für das jeweilige Mitglied des IR-Teams enthalten: Man muss verstehen können, anhand welcher Kriterien das IR-Playbook Anwendung findet und welche Maßnahmen zur Analyse, Eindämmung, Bereinigung und Wiederherstellung zu treffen sind. Je nach Szenario gibt es viele „Abzweigungen“ – abhängig davon, welche Informationen im Verlauf der Bearbeitung aufgedeckt werden. Mit zu bedenken: Die Phasen der Analyse, Eindämmung und Bereinigung finden oft parallel statt.

Ein IR-Playbook kann als eine Art Checkliste, als ausführliches Dokument oder als Prozessablaufdiagramm erstellt werden – die sinnvollste Form hängt von den persönlichen Präferenzen und der Arbeitsweise des IR-Teams ab. Wenn am Ende der Bearbeitung eines Vorfalls festgestellt wird, dass bestimmte Schritte im IR-Playbook nicht

wie geplant funktioniert haben, sollten diese Erkenntnisse in das IR-Playbook zurückfließen. Dadurch wird sichergestellt, dass die vorhandenen IR-Playbooks die Erfahrungen aus vergangenen Vorfällen widerspiegeln.

Meta-Checklisten für IR

Übergeordnet zu IR-Playbooks können Meta-Checklisten dabei unterstützen, den Gesamtüberblick im Bereich Incident-Response zu behalten: Mit deren Hilfe lassen sich sowohl die beschriebenen Vorbereitungsmaßnahmen kontrollieren als auch konkret alle relevanten Aspekte eines Vorfalls im Auge behalten.

Als Denkanstoß können zum Beispiel folgende Punkte für eine übergeordnete Checkliste herangezogen werden:

- _____ Wurde eine übergeordnete IR-Strategie eingeführt?
- _____ Wurden alle kritischen Systeme, Daten und Prozesse erfasst?
- _____ Sind alle Rollen und Verantwortlichkeiten im Kontext Incident-Response geklärt?
- _____ Wurden IR-Playbooks für typische Szenarien erstellt?
- _____ Wurden die technischen Voraussetzungen für die effiziente Erkennung und Bearbeitung eines Vorfalls umgesetzt?
- _____ Sind die Kommunikationswege bekannt und definiert?
- _____ Wurde ein externer Dienstleister für Incident-Response ausgewählt und alle Modalitäten geklärt?
- _____ Sind alle Kontaktdaten bekannt (Datenschutz, Behörden etc.)?

Für den Überblick über Aufgaben während der Vorfalls-Bearbeitung lassen sich zum Beispiel folgende Aspekte abfragen:

- _____ Wurde der Vorfall korrekt kategorisiert?
- _____ Wurden alle Interessensgruppen/Parteien informiert?
- _____ Wurden die Maßnahmen zur Eindämmung umgesetzt?
- _____ Wurden die Maßnahmen zur Bereinigung umgesetzt?
- _____ Wurden die Maßnahmen zur Wiederherstellung umgesetzt?
- _____ Wurde die Ursache des Vorfalls erkannt?
- _____ Wurde das Ausmaß des Vorfalls erkannt?
- _____ Wurden alle Meldepflichten eingehalten?
- _____ Wurden alle Schritte nachvollziehbar dokumentiert?
- _____ Wurde am Ende des Vorfalls eine Lessons-Learned-Runde durchgeführt?
- _____ Sind die Ergebnisse aus der Lessons-Learned-Runde wieder in die IR-Playbooks eingeflossen?

Fazit

Cyberangriffe lassen sich nicht immer verhindern, aber eine gut vorbereitete Incident-Response-Strategie kann ihre Auswirkungen minimieren: Sicherheitsvorfälle lassen sich durch eine gute Vorbereitung schneller, strukturierter und erfolgreich abschließen.

Unternehmen sind sehr gut beraten, viel Zeit in die Vorbereitungsmaßnahmen zu investieren. Neben organisatorischen Aspekten gehören dazu technische Maßnahmen, die fortlaufende Schulung des IR-Teams und die Erstellung von IR-Playbooks. Führt man darüber hinaus regelmäßig Übungen durch, kann das IR-Team im Ernstfall schnell und professionell auf Cyberangriffe reagieren. ■

Joshua Tiago arbeitet als Leitender Berater bei cirosec GmbH. Er leitet das IR-Team von cirosec und unterstützt Kunden bei der Bewältigung von Sicherheitsvorfällen.

Literatur

[1] International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), Information technology — Information security incident management, Part 1: Principles and process, ISO/IEC 27035-1:2023, Februar 2023, www.iso.org/standard/78973.html (kostenpflichtig)

[2] National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC), Computer Security Incident Handling Guide, NIST Special Publication SP 800-61 Rev. 2, August 2012,

<https://csrc.nist.gov/pubs/sp/800/61/r2/final> bzw. <https://doi.org/10.6028/NIST.SP.800-61r2>

[3] National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC), Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, NIST Special Publication SP 800-61 Rev. 3, April 2025, <https://csrc.nist.gov/pubs/sp/800/61/r3/final> bzw. <https://doi.org/10.6028/NIST.SP.800-61r3>