
Praxistipps IT

Cybersecurity in der Praxis

Risiken, Präventionsmaßnahmen,
Krisenmanagement

Krüger/Trappe/Samrock
2. Auflage, inklusive Downloads



IDW VERLAG GMBH

Ihr Zugang zum Download-Bereich von „Cybersecurity in der Praxis“ (2. Auflage)

Folgende Schritte sind zur Registrierung und Nutzung erforderlich:

1. Melden Sie sich mit Ihren Zugangsdaten im IDW Internetportal an.
Falls Sie noch keine Zugangsdaten besitzen, führen Sie bitte zunächst eine Erstregistrierung durch.
2. Unter **www.idw-verlag.de > Produkt Updates > Cybersecurity in der Praxis 2. Auflage** geben Sie bitte anschließend den unten abgedruckten Freischaltcode in die dafür vorgesehene Box ein.

Nun stehen Ihnen nach jedem Einloggen die Dateien zum Download zur Verfügung.

Freischalt-Code:

Praxistipps IT

Cybersecurity in der Praxis

Risiken, Präventionsmaßnahmen,
Krisenmanagement

Krüger/Trappe/Samrock
2. Auflage



IDW VERLAG GMBH

Das Thema Nachhaltigkeit liegt uns am Herzen:



Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne vorherige schriftliche Einwilligung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verbreitung in elektronischen Systemen. Es wird darauf hingewiesen, dass im Werk verwendete Markennamen und Produktbezeichnungen dem marken-, kennzeichen- oder urheberrechtlichen Schutz unterliegen. Die automatisierte Analyse des Werkes, um daraus Informationen insbesondere über Muster, Trends und Korrelationen gemäß § 44b UrhG („Text und Data Mining“) zu gewinnen, ist untersagt.

© 2025 IDW Verlag GmbH, Roßstraße 74, 40476 Düsseldorf (post@idw-verlag.de)

Die IDW Verlag GmbH ist ein Unternehmen des Instituts der Wirtschaftsprüfer in Deutschland e. V. (IDW).

Satz: Reemers Publishing Services GmbH, Krefeld
Druck und Bindung: C.H.Beck, Nördlingen
KN 12565

Die Angaben in diesem Werk wurden sorgfältig erstellt und entsprechen dem Wissensstand bei Redaktionsschluss. Da Hinweise und Fakten jedoch dem Wandel der Rechtsprechung und der Gesetzgebung unterliegen, kann für die Richtigkeit und Vollständigkeit der Angaben in diesem Werk keine Haftung übernommen werden. Gleichfalls werden die in diesem Werk abgedruckten Texte und Abbildungen einer üblichen Kontrolle unterzogen; das Auftreten von Druckfehlern kann jedoch gleichwohl nicht völlig ausgeschlossen werden, so dass für aufgrund von Druckfehlern fehlerhafte Texte und Abbildungen ebenfalls keine Haftung übernommen werden kann.

ISBN 978-3-8021-3206-3

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://www.d-nb.de> abrufbar.

Coverfoto: www.istock.com/matejmo

www.idw-verlag.de

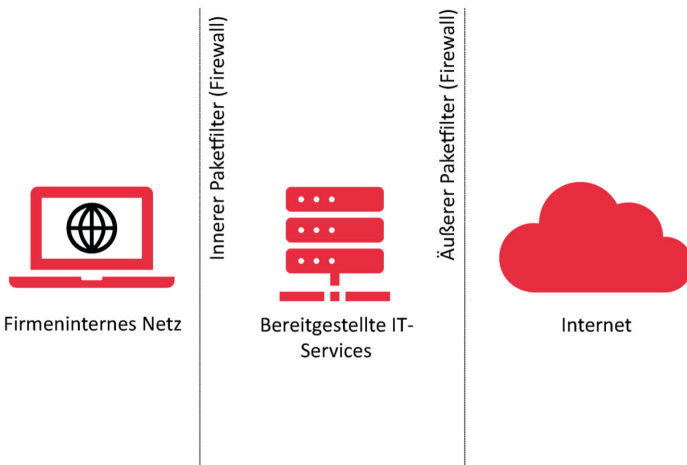


Abb. 2.4 Basisansatz für den Aufbau einer DMZ

„Abb. 2.4 Basisansatz für den Aufbau einer DMZ“ zeigt sehr stark vereinfacht das Prinzip einer DMZ. Dabei kommen zwei Paketfilter (Firewalls, siehe Kapitel 2.3.1) zum Einsatz, einer gegenüber dem Internet und einer gegenüber dem eigenen Firmennetz. Dazwischen herrscht eine Demilitarisierte Zone (DMZ), in der sehr strikte Vorgaben bezüglich des erlaubten Datenverkehrs gelten.

Ziel ist, dass IT-Services, die innerhalb einer Organisation oder nach außen erbracht werden, in einem geschützten Raum stehen. Bei einem Befall einzelner Clients im Firmennetz wird so verhindert, dass der Schadcode zentrale Rechenzentrumsinfrastruktur befällt, z.B.:

- Anmelde- und Verzeichnisdienste (Active Directory)
- Serverbetriebssysteme
- Virtualisierungsumgebungen
- Managementkomponenten für das Unternehmensnetzwerk
- Voice-over-IP Callmanager

Dieses sehr einfache Prinzip in der Praxis sicher und gut umzusetzen, erfordert jedoch erhebliche Planungen und hohen Aufwand bei der Konfiguration der einzelnen Komponenten. Zudem ist der Betrieb von zwei Firewalls (die idealerweise von zwei verschiedenen Herstellern stammen) in der Praxis nur für größere Betriebe handhabbar.

Krisenbewältigung

Trotz aller Präventionsmaßnahmen kann es zum Worst Case kommen. Mittels guter Vorbereitung können Auswirkungen abgeschwächt und ein Regelbetrieb schneller wiederhergestellt werden. Besonders durchgeführte Tests mit Betriebsunterbrechung schaffen bei der Krisenbewältigung notwendige Handlungssicherheit.

Auch wenn es bei der Abarbeitung einer Krise kein einheitliches Vorgehen gibt, so lässt sich der Ablauf („Abb. 3.3 Modell Auswirkungen eines Notfalls mit und ohne Vorwarnung“) prototypisch darstellen:

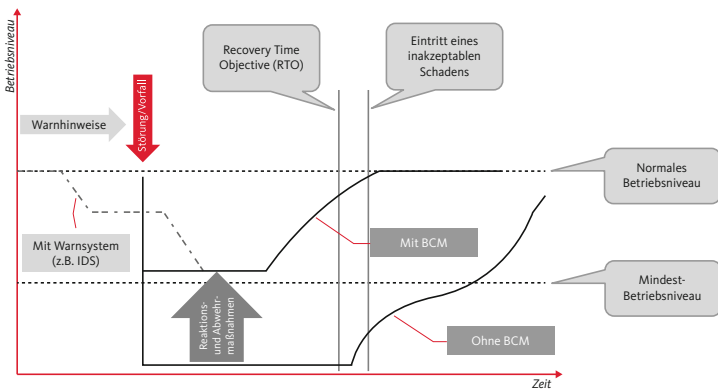


Abb. 3.3 Modell Auswirkungen eines Notfalls mit und ohne Vorwarnung

Ein Vorfall oder eine Störung kann sich schon vorher ankündigen oder auch abrupt auftreten. Gegebenenfalls haben schon Anzeichen wie Performance-Einbrüche, ein ungewöhnliches Antwort-Zeit-Verhalten oder andere Anzeichen einen Vorfall angekündigt.

Ohne etabliertes BCMS fällt das Betriebsniveau beim Eintritt einer Störung in der Regel erst einmal völlig ab. Ein gutes BCMS hat Reaktions- und Abwehrmaßnahmen etabliert, die den Totalausfall verhindern und ein gewisses Mindestbetriebsniveau gewährleisten.

Infolge einer gut durchgeführten Business-Impact-Analyse sollten somit die kritischen Geschäftsprozesse weiterlaufen können, während die Notfallbewältigungsorganisation an der Wiederherstellung des normalen Betriebsniveaus arbeitet.



Abb. 4.1 Strategische Kommunikation während Sicherheitsvorfällen

Je nachdem, welche Daten oder Dienste von dem Angriff betroffen sind, kann es erforderlich sein, Behörden einzuschalten. Bei gravierenden Fällen ist eine frühzeitige Einbeziehung der Polizei – insbesondere von Cybercrime-Spezialabteilungen – sinnvoll, da diese bei Ermittlungen und forensischer Sicherung unterstützen können. Nicht selten wird außerdem das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder eine andere nationale Cybersicherheitsorganisation hinzugezogen. An dieser Stelle gilt es, die rechtlichen Vorschriften genau einzuhalten und auch in der Kommunikation nach außen sorgsam vorzugehen. Kunden, Partner oder die Presse möchten oft wissen, was passiert ist und wie lange etwaige Einschränkungen voraussichtlich andauern. Eine offene, klare und faktenbasierte Kommunikation hat sich in der Praxis als beste Strategie erwiesen, um Spekulationen und Misstrauen vorzubeugen.

4.3 Technische Incident Response

Während das Krisenmanagement die organisatorischen Fäden in der Hand hält, konzentriert sich das technische Incident-Response-Team auf die Analyse des Angriffs, das Containment und die Beseitigung der Bedrohung. Eine gründliche Log-Analyse ist dabei häufig der Ausgangspunkt, da Firewall- und Server-Logs, ebenso wie Anti-Virus-Benachrichtigungen oder Netzwerkmonitoring-Tools, erste Indizien über das Ausmaß und die Her-

kunft des Angriffs liefern. Besonders wichtig ist es, festzustellen, wie sich der Angreifer ins Netzwerk bewegen konnte und ob es bereits zu einem Datenabfluss gekommen ist.

Bei schwerwiegenden Vorfällen werden oft IT-Forensiker hinzugezogen, die mittels Memory-Forensik und Festplatten-Images Spuren sichern, um später den Tatverlauf zu rekonstruieren und gegebenenfalls gerichtlich verwerten zu können. Hierzu werden spezielle Tools eingesetzt, die beispielsweise laufende Prozesse im Arbeitsspeicher abbilden oder Hashwerte von Dateien und Partitionen vergleichen. Erkenntnisse dieser Analysen fließen in den laufenden Prozess ein, um kompromittierte Systeme zu isolieren, Schadsoftware zu beseitigen und Schwachstellen schnellstmöglich zu schließen.

Hat sich ein Angriff etwa über alte Softwareversionen oder ungepatchte Betriebssysteme verbreitet, so findet anschließend ein umfassendes Patch Management statt, bei dem Updates auf allen kritischen Systemen eingespielt werden. Zeitgleich wird häufig geprüft, ob sich bestimmte Ports, Dienste oder Protokolle (beispielsweise RDP, FTP oder unsichere Versionen von SMB) kurzfristig abschalten lassen, um die Angriffsfläche zu verringern. So soll nicht nur das unmittelbare Problem gelöst, sondern auch ein erneuter Angriff verhindert werden.

4.4 Koordination mit Behörden und Partnern

Ab einem gewissen Schweregrad ist die Zusammenarbeit mit öffentlichen Stellen unerlässlich. Kommt es etwa zu Erpressungsversuchen mit Ransomware oder zu großflächigen Ausfällen kritischer Infrastruktur, sollten Unternehmen umgehend Kontakt zu den entsprechenden Behörden aufnehmen. Die Polizei oder Staatsanwaltschaft kann den Vorfall juristisch einordnen und dazu raten, forensische Maßnahmen zu ergreifen, die später für eine Anzeige oder ein Strafverfahren relevant sind. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet im Falle massiver Störungen Unterstützung an.

Parallel dazu ist die Abstimmung mit betroffenen Partnern oder Kunden ein elementarer Bestandteil der Reaktion. Wenn Kundendaten durch den Vorfall kompromittiert wurden, kann der Schaden für das Unternehmen nicht nur finanziell, sondern auch reputationsbedingt enorm sein. Offene und kompetente Kommunikation trägt dazu bei, dass Partner ihrerseits Schutzmaßnahmen ergreifen können, beispielsweise Passwörter ändern



IDW VERLAG GMBH

ISBN 978-3-8021-3206-3
Preis: 54,00 € (D)
www.idw-verlag.de

