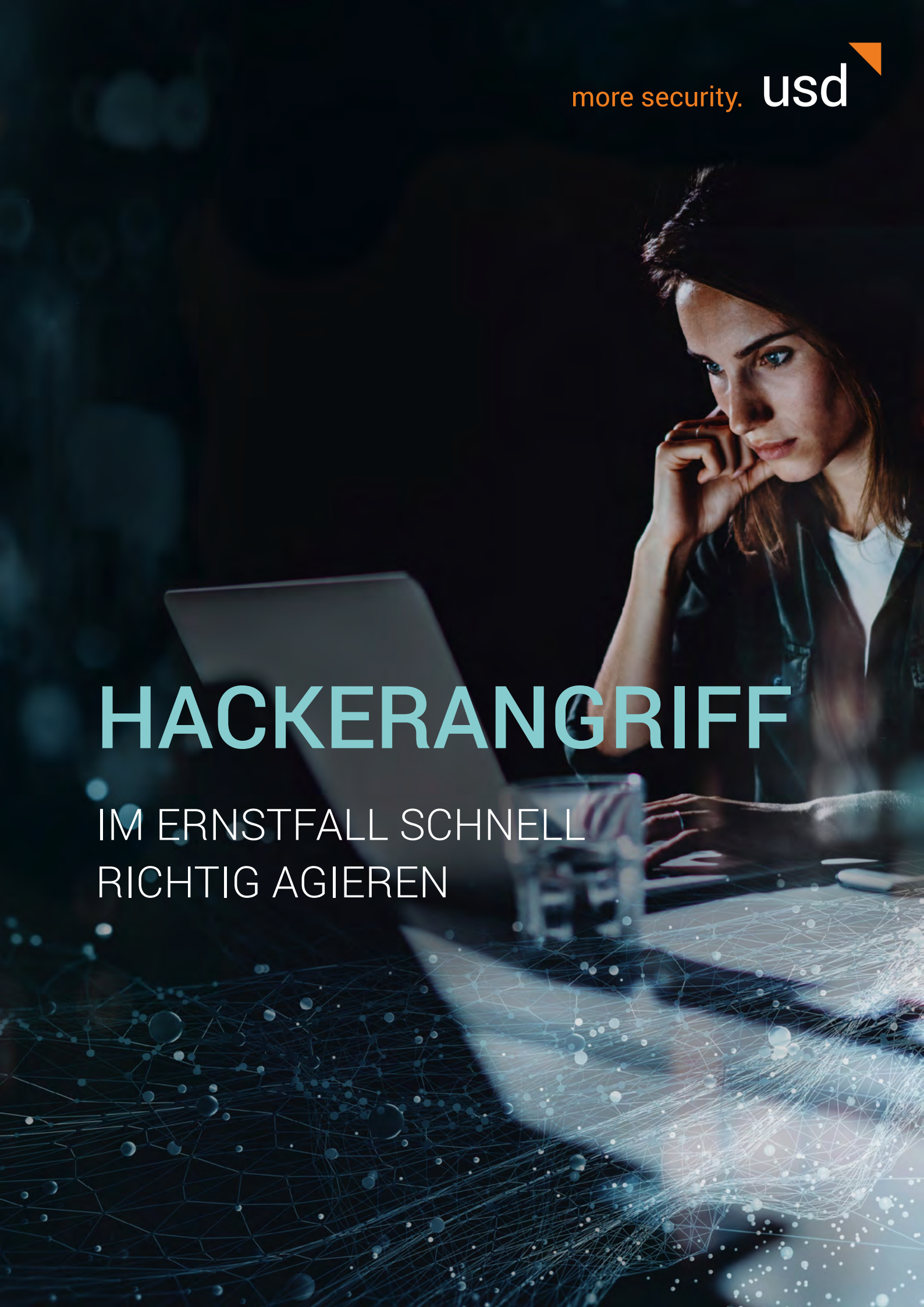
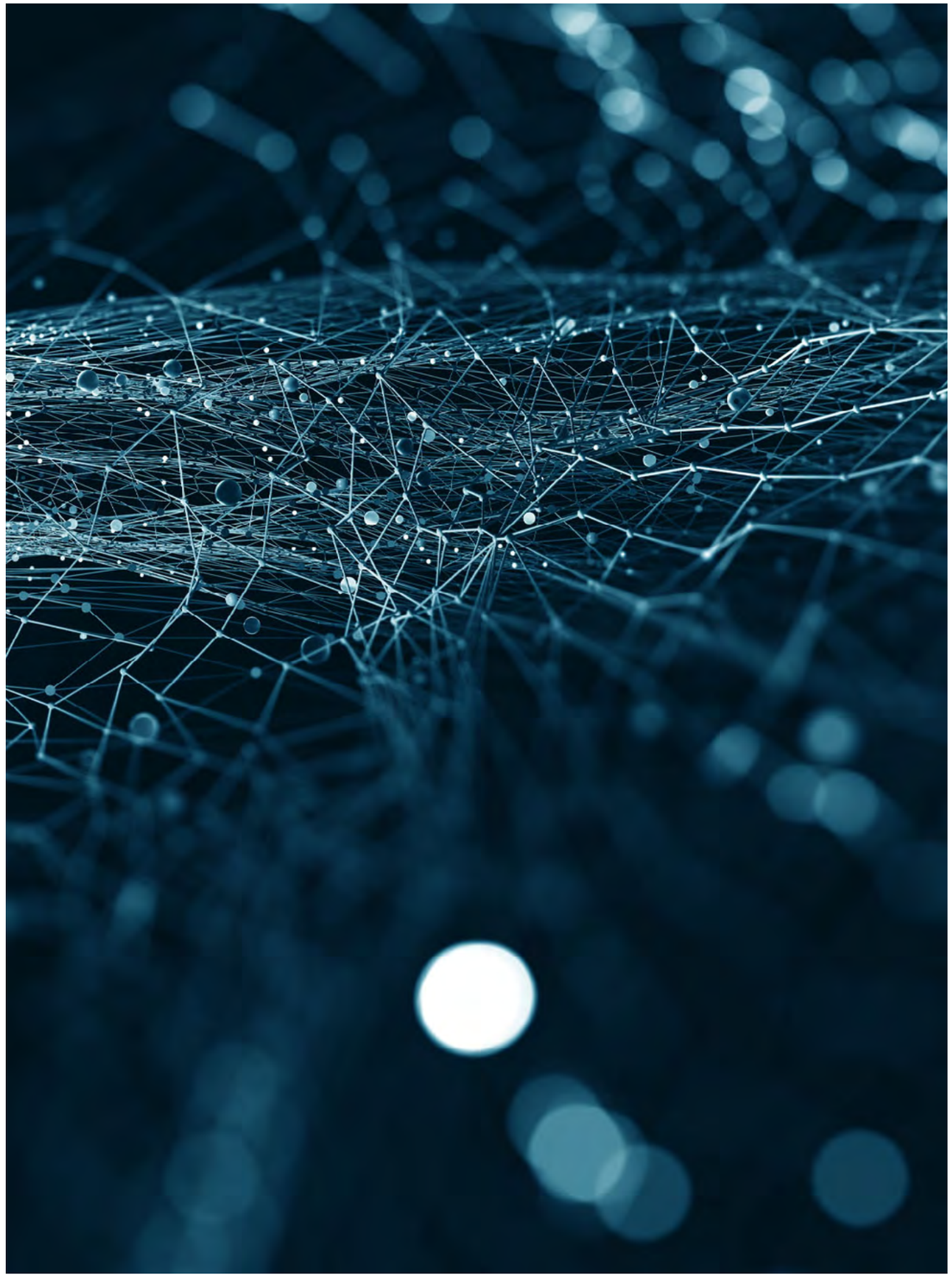

more security. usd
HACKERANGRIFF
IM ERNSTFALL SCHNELL
RICHTIG AGIEREN



Cyberattacken: ein existenzbedrohendes Risiko für Ihr Unternehmen

Egal ob Phishing-E-Mail, Malware, ungewöhnliche Aktivitäten auf dem Desktop oder verdächtige Logeinträge und Verhaltensmuster auf Servern oder im Netzwerk: ein Cyberangriff führt zu einer hohen Belastung bei betroffenen Mitarbeitern, Administratoren sowie verantwortlichen Managern und der Geschäftsführung.

Wird ein Cybervorfall von Mitarbeitern aus Angst vor persönlichen Konsequenzen bewusst verheimlicht oder aus Unwissenheit schlicht nicht erkannt, können sich Hacker ungehindert in Ihrem Unternehmen digital ausbreiten.

In der Folge maximieren sich die Schäden: vertrauliche Daten werden entwendet, IT-Systeme werden sabotiert und müssen neu aufgesetzt werden, Mitarbeiter können ihrer Arbeit nicht mehr nachkommen, Kundenaufträge sind gefährdet. Kurz darauf drohen Imageschäden und Vertrauensverlust bei Partnern. Für Unternehmen wird ein erfolgreicher Hackerangriff damit schnell zu einer existenzbedrohenden Ausnahmesituation.

Aus diesen Gründen ist die Schulung der Mitarbeiter und eine richtige und schnelle Reaktion aller Beteiligten bei einem Cybersicherheitsvorfall von entscheidender Bedeutung. Nur so können Angreifer rechtzeitig gestoppt, die Folgen begrenzt und eine Analyse des Vorfalls mit anschließender Korrektur der Ursachen ermöglicht werden.

Deshalb unser Tipp: genau wie Sie sich persönlich mit den Fluchtwegen in Ihrem Büro vertraut machen und Ihr Unternehmen durch Brandmeldeanlagen gegen Feuer absichern, schützt Sie eine gezielte Vorbereitung auf einen Cyberangriff vor falschen Reaktionen und verbessert damit Ihre Chancen im Ernstfall den Schaden zu minimieren.

Den ersten Schritt dafür haben Sie bereits gemacht: auf den folgenden Seiten erläutern wir Ihnen, wie Sie bei einem Hackerangriff korrekt vorgehen, ganz persönlich und als Unternehmen. Wir empfehlen Ihnen, unseren Flyer griffbereit zu halten. Sollte es zu einem Cybervorfall kommen, haben Sie so die Informationen im schnellen Zugriff.

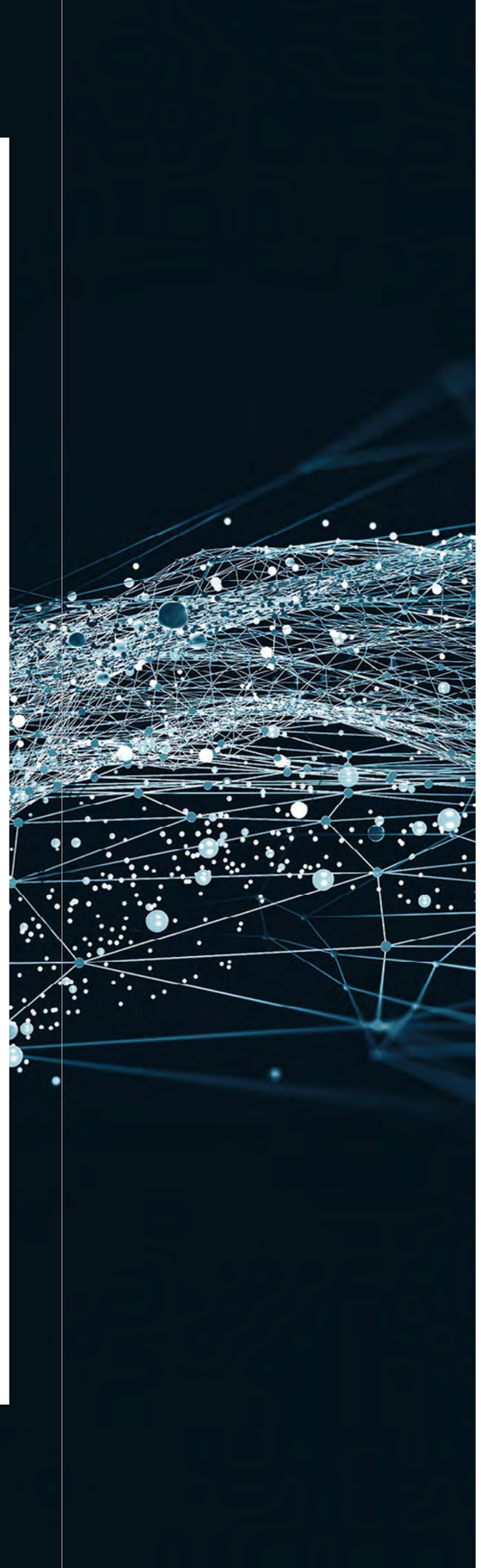
Bestmöglicher Schutz vor Hackerangriffen

Um sicherzustellen, dass Ihre Mitarbeiter im Ernstfall schnell richtig reagieren, sollte Ihre Organisation einen Incident-Response-Plan etablieren. Hier werden Zuständigkeiten, relevante Gegenmaßnahmen sowie Kommunikationswege für die wichtigsten Angriffsszenarien definiert und festgeschrieben. Konkrete Inhalte haben wir auf den folgenden Seiten für Sie zusammengefasst.

Natürlich hilft der beste Notfallplan nichts, wenn ihn Ihre Mitarbeiter nicht kennen. Aus diesem Grund ist es unbedingt notwendig, dass alle Mitarbeiter über den Incident-Response-Plan und seine Inhalte regelmäßig informiert werden. Ob dies per (online) Schulung, Newspost im Intranet oder per Infomail geschieht, obliegt dabei ganz Ihnen. Um die Wirksamkeit des Incident-Response-Plans sicherzustellen, sollten Sie außerdem mindestens einmal im Jahr im Rahmen einer Angriffssimulation die Umsetzung in der Realität testen.

Mit dem Incident-Response-Plan stellen Sie sicher, dass Ihre Organisation für den Ernstfall vorbereitet ist. Um aber den Hackerangriff überhaupt zu bemerken sowie nachvollziehen und adäquat reagieren zu können, empfehlen wir unbedingt Ihre IT-Systeme zu inventarisieren und ein stringentes Logging, Monitoring und Alerting umzusetzen.

Im Idealfall kommt es nie zu einem erfolgreichen Hackerangriff. Um die Wahrscheinlichkeit einer erfolgreichen Kompromittierung zu reduzieren, empfehlen wir Ihnen neben dem Einsatz von Antivirenprogrammen, einer sicheren Systemkonfiguration nach Best Practices zum Beispiel vom CIS und einer Netzwerksegmentierung auch die Durchführung regelmäßiger Schwachstellenscans und Pentests. So identifizieren Sie Schwachstellen in Ihren IT-Systemen proaktiv, bevor sie von einem Angreifer ausgenutzt werden können. Darüber hinaus sollten Mitarbeiter regelmäßig für die Gefahren eines Cyberangriffs sensibilisiert und ausführlich darüber informiert werden.



Verhaltensregeln für den Ernstfall

Nachfolgend haben wir für Sie einige Verhaltensregeln für den Ernstfall eines Hackerangriffs vorbereitet. Wir unterscheiden dabei verschiedene Rollen: einzelne Benutzer, die IT, das Management und das Unternehmen. Für jede Rolle finden Sie jeweils dedizierte Ratschläge.

VORBEREITUNG AUF DEN ERNSTFALL

Incident Readiness

- Incident Response Plan: Zuständigkeiten & Meldewege definieren
- Awareness schaffen
- Logging, Monitoring & Alerting
- Regelmäßige Sicherheitsanalysen

VORGEHEN BEI SICHERHEITSVORFÄLLEN

MITARBEITER

Vorfälle erkennen & richtig agieren

- Ruhe bewahren
- Veränderungen vermeiden
- Melden

EXTERNE IT-FORENSIKER

Technische Analyse

- Beweissicherung
- Forensische Analyse & Vorfall rekonstruieren
- Angreifer isolieren & aussperren

TEAM

Lessons Learned

- Incident Response Plan anpassen
- Verbesserungspotential identifizieren, Umsetzung planen
- regelmäßige Sicherheitsanalysen

INTERNE IT & MANAGEMENT

Schnelle Reaktion

- Verifizieren & Eskalieren
- Beweise sichern
- Verantwortliche bestimmen
- (Externe) Sachverständige hinzuziehen
- Kommunikation abstimmen, Meldepflichten beachten

IT & MANAGMENT

Back to Business

- Schwachstellen schließen
- Systeme & Daten wiederherstellen
- interne & externe Kommunikation

MITARBEITER

Ein Mitarbeiter stellt einen IT-Sicherheitsvorfall fest, beispielsweise, weil er direkt im Rahmen eines Phishing Angriffs betroffen ist, oder weil ihm ein ungewöhnliches Verhalten auf IT-Systemen oder im Netzwerk des Unternehmens auffällt.

1 Bewahren Sie Ruhe

Vermeiden Sie impulsive Reaktionen oder Panik, denn unkoordinierte Handlungen können wertvolle Beweise vernichten. Nehmen Sie sich einen Moment Zeit, um sich erneut mit dem Incident-Response-Plan vertraut zu machen und über die nächsten Schritte nachzudenken, bevor Sie agieren.

2 Verändern Sie das System nicht

Jede Veränderung am betroffenen System vernichtet wichtige Spuren und erschwert dadurch die Ursachenforschung. Deshalb ist es wichtig, Änderungen so gering wie möglich zu halten, bis mit einem Experten Rücksprache gehalten wurde. Anschließend kann es sinnvoll sein, das System vom Netzwerk zu trennen (Kabel & kabellose Verbindungen). Besonders wichtig: schalten Sie das System nicht aus, da hierdurch Informationen über gestartete Systemprozesse und den Inhalt des Arbeitsspeichers verloren gehen.

3 Melden Sie den Sicherheitsvorfall umgehend

Informieren Sie sich am besten im Vorfeld über den Incident-Response-Plan in Ihrer Organisation und befolgen Sie diesen im Ernstfall. Melden Sie einen Vorfall umgehend an die dafür vorgesehene interne Anlaufstelle, meist Ihre hausinterne IT. Beschreiben Sie dabei möglichst genau, was Sie beobachtet haben.

4 Dokumentieren Sie den Vorfall und Ihr Vorgehen

Halten Sie genau fest, was sich wann ereignet hat, welche Maßnahmen Sie getroffen haben und wer Zugriff zum betroffenen System hatte. Notieren Sie sich, wer ab dem Zeitpunkt (der Erkennung) des Angriffs an den kompromittierten Systemen welche Änderungen vorgenommen hat. Diese Informationen sind später für die Aufarbeitung des Vorfalls wichtig.

INTERNE IT & MANAGEMENT

Ein Mitarbeiter meldet einen IT-Sicherheitsvorfall vorschriftsmäßig. Die interne IT und das Management leiten notwendige Gegenmaßnahmen ein.

1 Schnelle Reaktion

Sicherheitsvorfälle erfordern eine schnelle, aber koordinierte Reaktion und haben daher oberste Priorität. Führen Sie zuerst eine Bewertung der Situation durch, um sicherzustellen, dass es sich tatsächlich um einen Sicherheitsvorfall handelt und ein technischer Defekt ausgeschlossen werden kann. Gab es zum Beispiel weitere Meldungen im Unternehmen, sind weitere Systeme betroffen, laufen untypische Prozesse oder wurden Netzwerkverbindungen zu ungewöhnlichen Domains registriert. Mit speziellen Tools wie dem THOR-Scanner der Firma Nextron lässt sich außerdem sehr schnell feststellen, ob ein System im Rahmen eines Hackerangriffs kompromittiert wurde. Bestätigt sich nach der ersten Analyse der Verdachtsfall, greift der Incident-Response-Plan und die hier festgelegten Schritte sind umzusetzen.

2 Analyse und Bewertung des Vorfalls

Legen Sie einen Verantwortlichen für den Sicherheitsvorfall fest, der die weiteren Schritte koordiniert und leitet. Stellen Sie sicher, dass alle Informationen zentral erfasst werden. Nun gilt es Folgendes zu klären: welche Systeme und Daten sind von dem Sicherheitsvorfall betroffen? Ist der Angreifer noch aktiv? Wenn ja, sollten Maßnahmen eingeleitet werden, um die Auswirkungen zu begrenzen, zum Beispiel indem die betroffenen Systeme isoliert und Passwörter geändert werden. Dennoch sollten Veränderungen so gering wie möglich gehalten werden. Ziehen Sie dazu (externe) Experten, wie IT-Forensiker hinzu, die Ihnen bei der Bewertung helfen und eine forensische Analyse der betroffenen Systeme vornehmen.

3 Abstimmung der Kommunikation

Informieren Sie die relevanten Stellen nach dem Need-to-Know-Prinzip über den Vorfall und stimmen Sie das weitere Vorgehen ab – idealerweise über kurze Meldewege. Abhängig vom Ausmaß des Vorfalls müssen die Unternehmensleitung, Rechtsabteilung, Personalabteilung, ISO-Organisation, Datenschutzbeauftrage und andere eingebunden werden. Durch Einbindung des Top-Managements können notwendige Mittel zur Rückkehr in den Normalbetrieb kurzfristig freigegeben werden. Beachten Sie bei der Kommunikation, dass der Angreifer ggf. Zugriff auf interne Kommunikationskanäle hat. Ziehen Sie rechtzeitig externe IT-Forensik Experten hinzu.

4 Meldepflicht bei Cyber-Versicherungen und Behörden

Melden Sie den Angriff zeitnah Ihrer Cyber-Versicherung, sofern Sie über eine Cyber-Police verfügen, da häufig Meldefristen greifen. Die Versicherungsgesellschaft wird Sie dann über das weitere Vorgehen informieren. Prüfen Sie zudem, ob der Angriff einer behördlichen Meldepflicht unterliegt.

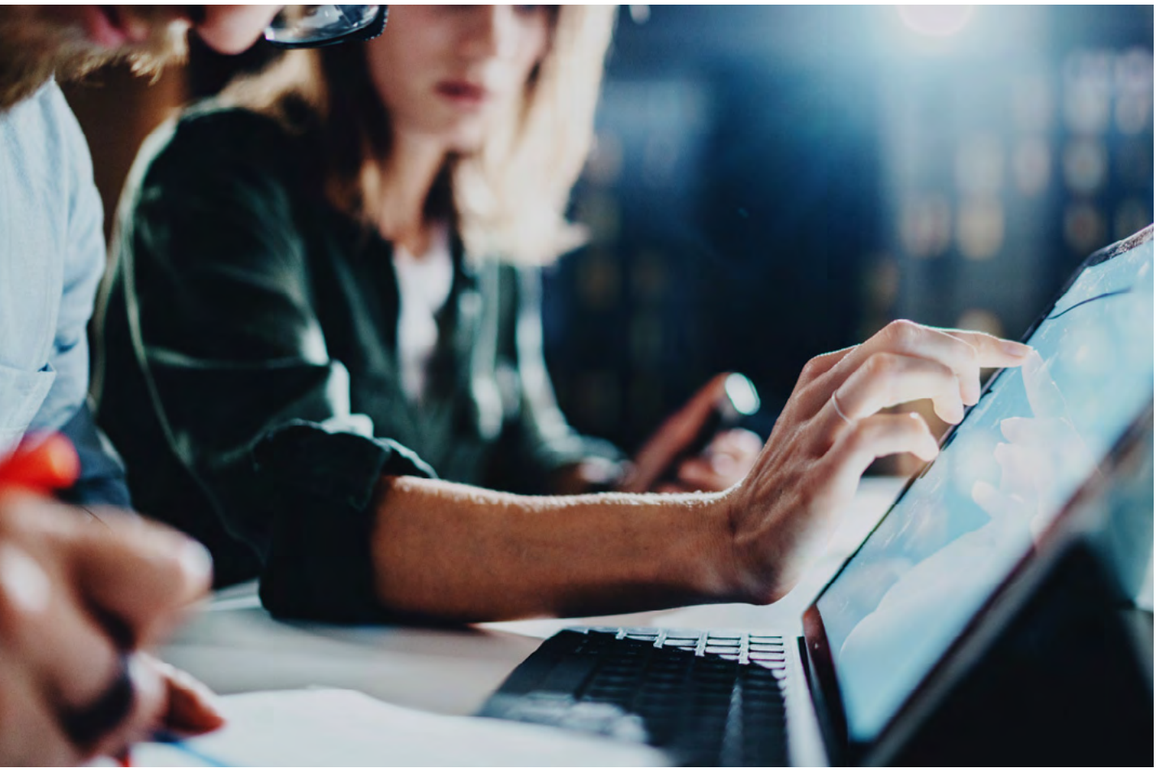
5 Erfassung der Beweise

Sichern Sie alle Beweise des Angriffs für eine IT-forensische Untersuchung. Dazu gehören System-Protokolle, Logfiles, Festplatten-Images betroffener Systeme, Netzwerk-Traffic, Notizen usw. Zudem kann bei betroffenen Systemen der Arbeitsspeicher (RAM) von entscheidender Bedeutung sein. Die Art der Beweissicherung hängt vom jeweiligen System ab (zum Beispiel können bei virtualisierten Systemen RAM und Festplatten-Image i.d.R. sehr leicht gesichert werden) und sollte stets nach forensischen Best-Practices und in Rücksprache mit (oder sogar durch) IT-Forensik Experten erfolgen. Sichern Sie Logfiles zeitnah um sicherzustellen, dass diese nicht automatisch gelöscht oder überschrieben werden.

(EXTERNE) IT-FORENSIK-SACHVERSTÄNDIGE

Im Rahmen der ersten Analyse wird ein Cybersicherheitsvorfall bestätigt. Das betroffene Unternehmen beauftragt einen spezialisierten IT-Forensik-Experten, der die gesicherten Beweise analysiert und eine abschließende Bewertung inklusive Handlungsempfehlungen unterbreitet.

Auf Basis der gesammelten Daten Ihrer potenziell betroffenen Systeme erfolgt eine detaillierte IT-forensische Untersuchung. Sollten dabei Anhaltspunkte für weitere betroffene Systeme identifiziert werden, müssen erneut Daten gesammelt und ausgewertet werden. Nach Abschluss der Datenanalyse erfolgt die formale Dokumentation der Untersuchungsergebnisse. Diese sollten in einem Bericht aufgearbeitet werden und sowohl eine Bewertung des Vorfalls für das Management als auch technische Details der Untersuchung enthalten.



NACH DEM SICHERHEITSVORFALL

Abhängig von der Art des Sicherheitsvorfalls können nun unterschiedliche Schritte für das betroffene Unternehmen sinnvoll und notwendig sein.

1 Identifizierte Probleme beheben

Wenn die IT-forensische Untersuchung technische Sicherheitslücken als Ursache für den Vorfall identifiziert hat, ist es wichtig diese schnellstmöglich zu korrigieren. Die Behebung sollte durch IT-Sicherheits-Experten verifiziert werden. Andernfalls kann eine erneute Kompromittierung nach der Bereinigung der Systeme nicht ausgeschlossen werden.

2 Bereinigung der Systeme und Wiederherstellung

Nachdem sichergestellt ist, dass keine weiteren Bedrohungen existieren, können betroffene Systeme neu aufgesetzt, aus einem Backup wiederhergestellt oder bereinigt werden. Die Entscheidung hängt von den Erkenntnissen der Analyse ab. Überprüfen Sie anschließend, dass keine Schwachstellen vorhanden sind und behalten Sie die Systeme und Umgebungen im Blick.

3 Nutzen Sie den Sicherheitsvorfall als Lessons Learned

Im Rahmen der Nachbearbeitung haben Sie die Chance, verbesserungswürdige Abläufe und technische Maßnahmen zu identifizieren, um zukünftige Cyberangriffe zu verhindern. Erkenntnisse aus diesen Lessons Learned fließen in die Verbesserung Ihrer Incident-Response-Strategie ein.

UNSERE UNTERSTÜTZUNGS-LEISTUNGEN

Sind Sie auf den Ernstfall vorbereitet?

Wir begleiten Sie bei bei der Ausarbeitung des Incident-Response-Plans und der Umsetzung passender Schutzmaßnahmen, um einen Hackerangriff zu verhindern.

Haben Sie einen Verdacht?

Wir helfen Ihnen schnell und unkompliziert bei der Bewertung der Situation.

Sie wurden Opfer eines Cyberangriffs?

Unser Team aus erfahrenen IT-Forensikern führt eine detaillierte Analyse des Vorfalls durch und berät Sie bei der weiteren Behandlung des Sicherheitsvorfalls.

Wir sind für Sie da!

Sprechen Sie uns an. Wir unterstützen Sie gerne jederzeit bei dem Schutz vor, der Vorbereitung auf und / oder der Begleitung eines IT-Sicherheitsvorfalls.

Daniel Heyne
Security Consultant Pentest,
OSCP, OSCE

E-Mail: kontakt@usd.de
www.usd.de

NOTFALL-HOTLINE
+49 6102 8631-190

usd AG
Frankfurter Str. 233, Haus C1
63263 Neu-Isenburg

Telefon: +49 6102 8631-0
Mail: kontakt@usd.de

www.usd.de