hvs consulting

10 Verhaltensregeln bei Sicherheitsvorfällen

Notfall-Rufnummer: + 49 (0)89 / 890 63 62 - 61
forensik@hvs-consulting.de

1. Bewahren Sie Ruhe! Unkoordinierte Handlungen könnten wertvolle Beweise vernichten.
2. Führen Sie eine anfängliche Beurteilung des Vorfalls durch.
3. Bei aktiven Angriffen: Begrenzen Sie den Schaden und trennen Sie die betroffenen Systeme vom Netzwerk.
4. Informieren Sie das Management.
5. Kontaktieren Sie externe IuK-Forensik Sachverständige.
6. Sichern Sie Beweismittel mit IuK-forensischen Werkzeugen.
7. Benachrichtigen Sie nach Rücksprache mit Ihrem Rechtsberater ggf. externe Stellen.
8. Führen Sie eine erste Analyse der gesicherten Beweise durch.
9. Stellen Sie ggf. die Systeme wieder her.
10. Lernen Sie aus Sicherheitsvorfällen.

1. Bewahren Sie Ruhe!
Vermeiden Sie Überreaktionen oder Panik. Befolgen Sie systematisch Ihren definierten Incident Response Plan. Unkoordinierte Handlungen (z.B. Neustarten von Rechnern oder An- bzw. Abmeldung) könnten wertvolle Beweise vernichten. Verwenden Sie Out-of-Band-Kommunikationsmittel, wie z. B. Telefon und Fax, oder sprechen Sie persönlich mit den betreffenden Personen. Angreifer können sonst möglicherweise mithören.

2. Führen Sie eine anfängliche Beurteilung durch.
Legen Sie eine anfängliche Prioritätsebene fest, und bestimmen Sie für den Sicherheitsvorfall einen Verantwortlichen. Ermitteln Sie die Art und das Ausmaß des Vorfalls, z.B. Abfluss von vertraulichen Informationen (fahrlässig oder Vorsatz), Wirtschaftskriminalität & Betrug (z.B. Manipulation bzw. Abfluss von Informationen), Missbrauch von IuK-Systemen (z.B. Bad-Admin, strafrechtlich relevante Inhalte) oder gezielte Hacking-Angriffe (z.B. Advanced Persistence Threats, Denial of Service), etc.
Identifizieren Sie alle von dem Vorfall betroffenen Systeme. Denken Sie auch an mobile Geräte (z.B. SmartPhone & Tablets etc.) und „Sonder- bzw. Spezial-Systeme" (z.B. Telefonanlage/VoIP-System, Produktionssysteme, Multifunktionsgeräte wie Netzwerkdrucker, Zutrittskontrollsystem etc.).

3. Bei aktiven Angriffen: Begrenzen Sie den Schaden.
Isolieren Sie bei aktiven Angriffen die betroffenen Systeme, indem Sie diese vom Netzwerk trennen. Sollte dies z.B. im Fall von hochverfügbaren Serversystemen nicht möglich sein, prüfen Sie die Möglichkeit, das System teilweise zu isolieren. Ändern Sie unbedingt die Passwörter von kompromittierten Benutzerkonten, insbesondere hochpriviligierten Accounts z.B. Admin/Root-Accounts, Service-Accounts, Technische Accounts. Achten Sie darauf, bei Ihren Aktionen keine Beweise zu vernichten. Betroffene Systeme sollten keinesfalls neugestartet werden.

4. Informieren Sie das Management.
Informieren Sie unternehmensintern alle relevanten Stellen (je nach Auswirkung & Bedeutung) des Sicherheitsvorfalls: (Top-) Management, Rechtsabteilung, Personalabteilung, Datenschutz, Fraud-Management, Revision, Compliance, Presseabteilung bzw. Abteilung für Öffentlichkeitsarbeit & -kommunikation, Betriebsrat. Halten Sie aber die Gruppe der involvierten Personen so klein wie möglich!

5. Kontaktieren Sie externe IuK-Forensik-Sachverständige.
Kontaktieren Sie bei Sicherheitsvorfällen neutrale, externe Sachverständige mit dem entsprechenden Fach-KnowHow und Referenzen.

6. Sichern Sie Beweismittel.
Führen Sie zeitnah eine forensische Sicherung der betroffenen IuK-Systeme auf dedizierten Sicherungsmedien durch. Wenn möglich, sollten Sie die IuK-Systeme vollständig sichern, einschließlich der flüchtigen Daten aus dem Arbeitsspeicher.

Beispiele für IuK-forensische Beweissicherung:
- Sicherung des Arbeitsspeichers der betroffenen Systeme: Verwenden Sie erprobte Tools (z.B. FTK Imager, F-Response, etc.). Ist kein administrativer Zugriff auf das System möglich, sollten Sie zumindest wesentliche Laufzeitinformationen dokumentieren (date, time, netstat, ps/tasklist etc.).
- Forensische Duplikation von persistenten Speichermedien (z.B. Festplatten, USB-Sticks, etc.): Verwenden Sie zertifizierte WriteBlocker Hardware. Kann eine Duplikation über Hardware ggf. aufgrund von Verschlüsselung oder verteilten Dateisystemen nicht gelesen werden, sollte zumindest eine Duplikation der Daten aus dem Live-System durchgeführt werden (z.B. FTK Imager, dd etc.).
- Forensische Sicherung von mobilen Geräten: Wenn möglich sollte ein volles Duplikat des Gerätespeichers erstellt werden. Ist dies aufgrund fehlender Schnittstellen nicht möglich (z.B. für iOS Geräte), kann eine Sicherung über die Backup-Schnittstelle erfolgen.
- Forensische Sicherung virtueller Systeme (z.B. VMWare/ESX, Hyper-V, XEN): Erstellen Sie Snapshot und Kopie des entsprechenden RAM- und HDD-Files.
- Logfiles: Sichern Sie relevante Logdaten von Ihrer Proxy-, Firewall- und AntiVirus-Infrastruktur. Denken Sie auch an die Netzlaufwerke und E-Mailkonten betroffener Personen. Möglicherweise ist auch das Zutrittskontrollsystem oder die Videoüberwachung relevant.

Wichtig: Dokumentieren Sie im Rahmen der Beweissicherung, wer die Beweismittel wie und wann gesammelt hat und wer darauf zugreifen konnte. Beachten Sie bei der Beweissicherung juristische Fallstricke (z.B. allgemeine Persönlichkeitsrechte, Mitbestimmungs- & Informationsrechte). Holen Sie sich bei der Beweismittelsicherung ggf. externe Unterstützung (siehe Punkt 5).

7. Benachrichtigen Sie ggf. externe Stellen.
Eruieren Sie zusammen mit Ihrem Rechtsberater, ob der Vorfall den Behörden (z.B. zuständige Aufsichtsbehörde, BSI bei KRITIS-Unternehmen, Strafverfolgung, Datenschutz etc.) zwingend zu melden ist. Ggf. können auch weitere behördliche Stellen (z.B. Verfassungsschutz/BSI, ACS Meldestelle für Vorfälle etc.) informiert werden.

8. Führen Sie eine erste Analyse der gesicherten Beweise durch.
Untersuchen Sie Logfiles nach ungewöhnlicher Aktivität. Führen Sie eine automatisierte Analyse der gesicherten Beweisobjekte durch erprobte Tools (z.B. APT Scanner THOR) durch. Untersuchen Sie, ob es Benutzerkonten mit unerlaubten, erweiterten Berechtigungen gibt. Weitergehende Analysen (z.B. Wiederherstellung gelöschter Daten, Analyse von Benutzeraktivitäten etc.) sollten nur mit entsprechendem Fach-KnowHow bzw. Unterstützung externer Spezialisten durchgeführt werden!

9. Stellen Sie ggf. die Systeme wieder her.
Überprüfen Sie ob aktuelle, nicht beschädigte Sicherungen existieren. Stellen Sie das/die betroffenen IuK-Systeme wieder her. Überprüfen Sie die Funktionen und stellen Sie sicher, dass im Zusammenhang mit der Schadensbegrenzung („quick & dirty") nicht andere Schwachstellen erzeugt wurden.

10. Lernen Sie aus Sicherheitsvorfällen.
Untersuchen Sie die Ursachen für den Sicherheitsvorfall und verbessern daraufhin Ihre Schutzmaßnahmen, um erneute Vorfälle und damit verbundene Angriffe in Zukunft zu verhindern. Überprüfen Sie Ihren Incident Response Plan und erweitern Sie diesen auf Basis der neu gewonnenen Erkenntnisse und Erfahrungen (Lessons Learned).

HvS-Consulting AG
Notfall-Rufnummer: +49 (0)89 / 890 63 62 - 61 • forensik@hvs-consulting.de