Notfallplan IT-Sicherheit

Vorgehen, Anzeige-/Meldepflichten und Ansprechpartner

Der deutschen Wirtschaft ist im Jahr 2022 ein Schaden von rund 203 Milliarden Euro durch Diebstahl von IT-Ausrüstung und Daten, Spionage und Sabotage entstanden. Nach dem aktuellen Bericht des Bundesamtes für Sicherheit in der Informationstechnik ist die Bedrohung im Cyber-Raum so hoch wie nie. Im Falle einer Attacke aus dem Internet müssen die Betroffenen unverzüglich handeln.

1 Vorgehen im Notfall

Oft ist das Schadensausmaß eines Datenverlusts davon abhängig, wie schnell und offen Schwierigkeiten kommuniziert werden. Es ist daher sinnvoll, einen unternehmensinternen Notfallplan zu erstellen, der im Fall der Fälle abgearbeitet werden kann. Der Notfallplan sollte mindestens Alarmierungspläne, Meldewege, Wiederanlauf-, Wiederherstellungs- und Geschäftsfortführungspläne, sowie alle wichtigen Informationen und Aufgabenzuordnungen der Mitglieder des Notfallteams enthalten. Es sollte ein Notfallbeauftragter benannt werden, der den Notfallmanagement-Prozess steuert und koordiniert.

1.1 Sachverhaltserfassung und Benachrichtigung der zuständigen Personen

Zunächst muss geprüft werden, ob es sich bei einer Störungsmeldung tatsächlich um einen Notfall handelt.

Können gespeicherte Dateien und Dokumente nicht geöffnet oder wiedergefunden werden, muss der IT-Sicherheitsbeauftragte des Unternehmens kontaktiert werden, ohne selbst Datenrettungsversuche zu unternehmen. Sobald der Beauftragte die Situation analysiert hat, kann er Maßnahmen zur Datenrettung einleiten. Zudem sollten die betroffenen Mitarbeiter informiert werden.

Wenn starke Indizien darauf hinweisen, dass Wirtschaftsspionage vorliegt, müssen schnellstmöglich alle Internetverbindungen der im Netzwerk befindlichen PCs gekappt werden, um einen weiteren Zugriff durch Kriminelle zu verhindern.

1.2 Systemüberprüfung

Bevor versucht wird, verlorene oder beschädigte Dateien zu retten, muss zunächst eine Überprüfung des gesamten Systems durch ein geeignetes und aktuelles Antiviren-Programm durchgeführt werden (vor Neustart des PCs!). Schlägt dieses Alarm und werden Schadprogramme wie Viren oder Trojaner gefunden, muss versucht werden, diese mit Hilfe des Programms zu beseitigen.

Anschließend müssen alle persönlichen und unternehmensinternen Daten auf einem externen Medium gesichert werden, um die aktuellen und virengeprüften Dateien später wieder zurückspielen zu können. Da man nach dem Fund von Schadprogrammen nicht weiß, welcher Schaden am System angerichtet wurde, ist das Einspielen einer kompletten Datensicherung oder eine Neuinstallation des Systems und die Änderung sämtlicher Passwörter für diesen PC zwingend erforderlich. Andernfalls läuft man Gefahr, dass die erkannten Schadprogramme zwar restlos entfernt worden sind, aber zwischenzeitlich das System so verändert haben, dass Dritte nun unbemerkt Zugang zum System erlangen können.

1.3 Einsatz von Datenrettungssoftware

Ist es nicht möglich, die benötigten Dateien über Datensicherungen wieder zu gewinnen, besteht die Option, spezielle Datenrettungs-Software einzusetzen. Hierbei ist zu beachten, dass sowohl kostenlose, als auch kostenpflichtige Software generell nur dann eingesetzt werden darf, wenn sie von einem seriösen Hersteller stammt und den richtigen Funktionsumfang aufweist. Zudem ist eine Datenrettungs-Software nicht für jeden Anwender sinnvoll.

Bei Auswahl und Einsatz der Software sollte ein IT-Fachmann zu Rate gezogen werden, da ein großes Risiko besteht, die Situation der Festplatte durch Softwareeingriffe dieser Art weiter zu verschlimmern, so dass spätere professionelle Datenrettungsversuche durch Dienstleistungsunternehmen nicht weiterhelfen.

Datenrettungsversuche sollten nie auf dem Original-Datenträger, sondern auf einer Kopie der Festplatte durchgeführt werden.

1.4 Einschalten von Spezialisten

In manchen Fällen hilft nur noch die professionelle Hilfe eines seriösen Datenrettungs-Unternehmens. Wichtig ist, vorher unbedingt ein Abbild des auf der Festplatte enthaltenen Inhalts zu erstellen. Auch hierbei helfen die auf Datenrettung spezialisierten Unternehmen.

Zudem sollte die Einschaltung von IT-Forensikern in Betracht gezogen werden, um die eventuelle Geltendmachung von Schadensersatzansprüchen gegen den Angreifer und ggf. den eigenen IT-Sicherheitsdienstleister abzusichern (ohne auf etwaige behördliche Ermittlungen angewiesen zu sein).

2 Fragenkatalog

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen Fragenkatalog entwickelt. Die in den zwölf als Fragen formulierten Punkten implizierten Maßnahmen dienen als Impuls und Hilfestellung bei der individuellen Bewältigung:

– Wurden erste Bewertungen des Vorfalls durchgeführt, um festzustellen, ob es sich um einen Cyber-Angriff oder lediglich um einen technischen Defekt handelt?

- Haben Sie kontinuierlich Ihre Maßnahmen abgestimmt, dokumentiert und an alle relevanten Personen und Verantwortlichen kommuniziert?
- Wurden System-Protokolle, Log-Dateien, Notizen, Fotos von Bildschirminhalten, Datenträger und andere digitale Informationen forensisch gesichert?
- Haben Sie stets die besonders zeitkritischen und damit vorrangig zu schützenden Geschäftsprozesse im Fokus gehabt?
- Wurden betroffene Systeme vom Netzwerk getrennt? Wurden Internetverbindungen zu den betroffenen Systemen getrennt? Wurden alle unautorisierten Zugriffe unterbunden?
- Wurden Backups gestoppt und vor möglichen weiteren Einwirkungen geschützt?
- Wurden Maßnahmen unternommen, um das gesamte Maß der Ausbreitung festzustellen? Wurden alle angegriffenen Systeme identifiziert?
- Wurden die beim Cyber-Angriff ausgenutzten Schwachstellen in Systemen oder (Geschäfts-) Prozessen durch relevante Maßnahmen adressiert und behoben?
- Wurden, nach Abstimmung, die Polizei oder relevante Behörden (Datenschutz, Meldepflichten, etc.) benachrichtigt?
- Wurden die Zugangsberechtigungen und Authentisierungsmethoden für betroffene (geschäftliche und ggf. private) Accounts überprüft (z.B. neue Passwörter, 2FA)?
- Wird das Netzwerk nach dem Vorfall weiter überwacht, um mögliche erneute Anomalien fest zustellen?
- Wurden die betroffenen Daten und Systeme wiederhergestellt oder neu aufgebaut?

3 Melde- und Anzeigepflichten

Gegebenenfalls muss kurzfristig reagiert werden mit Blick auf folgende Pflichten und Obliegenheiten:

- Bei Verlust von personenbezogenen Daten können gem. Art 33, 34 DS-GVO datenschutzrechtliche Anzeigepflichten gegenüber der Datenschutzaufsichtsbehörde und den betroffenen Datenberechtigten bestehen.

  Grundsätzlich muss das verantwortliche Unternehmen der Aufsichtsbehörde jede Datenschutzverletzung unverzüglich und möglichst innerhalb von 72 Stunden melden, nachdem dem Verantwortlichen die Verletzung bekannt wurde. Ausnahmsweise besteht dann keine Pflicht zur Meldung bei der Datenschutzaufsichtsbehörde, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten der von der Datenschutzverletzung betroffenen Personen führt. Hierfür ist aber das verantwortliche Unternehmen beweispflichtig.

  Hat eine Datenschutzverletzung darüber hinaus voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten betroffener Personen zur Folge (z. B. Identitätsdiebstahl, Rufschädigung, materieller oder immaterieller Schaden), muss das verantwortliche Unternehmen grundsätzlich die hiervon betroffenen Personen ohne unangemessene Verzögerung benachrichtigen. Ausnahmsweise kann von der Benachrichtigung abgesehen werden, wenn das verantwortliche Unternehmen Risiken für die betroffenen Personen durch geeignete technische und organisatorische Schutzmaßnahmen ausgeschlossen hat.

– Gehört das angegriffene Unternehmen zu einer so genannten kritischen Infrastruktur (KRITIS-Unternehmen aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden), müssen die folgenden Störungen unverzüglich an das BSI gemeldet werden (BSI – KRITIS-FAQ (bund.de)):

  – Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen geführt haben;
  – erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen führen können.

– Soll für den eingetretenen Schaden Versicherungsschutz in Anspruch genommen werden, obliegt es dem Unternehmen, eine unverzügliche (erste) Schadensanzeige an die Versicherung zu richten.

4 Institutionen und Ansprechpartner

Besteht Bedarf an externer Unterstützung, können Sie sich an nachfolgende Institutionen wenden.

4.1 Bayerisches Landeskriminalamt Zentrale Ansprechstelle Cybercrime (ZAC)

Wenn Sie Opfer eines Cyberangriffs geworden sind, sollten Sie sich zuerst an die Zentrale Ansprechstelle Cybercrime beim Bayerischen LKA wenden. Es wird aber nicht nur dann tätig, wenn es zu Betrugsversuchen oder sogar wirtschaftlichen Schäden gekommen ist, sondern auch im Bereich der Prävention. Es steht daher bayerischen Unternehmen generell als Ansprechpartner für Sicherheitsfragen zur Verfügung. Die ZAC ist verpflichtet, die zur Kenntnis gelangten Informationen vertraulich zu behandeln. Allerdings ist die ZAC als Strafverfolgungsbehörde verpflichtet, bei Verdacht einer Straftat von Amts wegen, somit auch ohne einer entsprechenden Anzeige des Betroffenen, Ermittlungsmaßnahmen einzuleiten.

Kontakt

Die Zentrale Ansprechstelle Cybercrime erreichen Sie unter
(089) 1212-3300 oder E-Mail: zac@polizei.bayern.de.

Weitergehende Informationen finden Sie unter:
Die Bayerische Polizei - Zentrale Ansprechstelle Cybercrime für die Wirtschaft in Bayern

4.2 Das Cyber-Allianz-Zentrum Bayern (CAZ)

Besteht der Verdacht auf Wirtschaftsspionage, sollten Sie sich zunächst an das Cyber-Allianz-Zentrum Bayern des Bayerischen Landesamtes für Verfassungsschutz (LfV) wenden. Neben Ermittlungen im forensischen Bereich unterstützt auch das CAZ in Bayern ansässige Unternehmen bei der Prävention und Abwehr von elektronischen Angriffen. Alle Anfragen werden absolut vertraulich behandelt.

Im Unterschied zur ZAK ist das Landesamt für Verfassungsschutz nicht an das strafprozessuale Verfolgungsprinzip gebunden und somit nicht verpflichtet, im Falle der Kenntniserlangung von einem strafrechtlich relevanten Sachverhalt Strafverfolgungsbehörden einzuschalten bzw. eine entsprechende Strafanzeige zu erstatten.

Im Schadensfall stehen beim CAZ die drei Säulen „Kommunikation“, „Forensik“ und „Bewertung“ zur Unterstützung des betroffenen Unternehmens bereit:

- Kommunikation nimmt die Meldung des Betroffenen auf, kommuniziert nach innen, gibt ein Feedback der Bewertung an den Betroffenen, führt eine Abschlussbesprechung durch und gibt Handlungsempfehlungen.
- Forensik analysiert den Schadcode.
- Bewertung interpretiert den Angriff im Kontext des aktuellen nachrichtendienstlichen Lagebildes, reichert das Lagebild mit den bereits vorliegenden Parametern an, anonymisiert den Sachverhalt vor Veröffentlichung und gibt gegebenenfalls Warnmeldungen heraus.

Kontakt

Die Erstbewertung des Sachverhalts erfolgt telefonisch. Hierzu hat das CAZ eine Hotline eingerichtet:
Tel.: (089) 31201-222
E-Mail: caz@lfv.bayern.de

Warnmeldungen des CAZ und weitergehende Informationen finden Sie unter:
http://www.verfassungsschutz.bayern.de/spionageabwehr/cyber_allianz_zentrum/index.html

4.3 Bundesamt für Sicherheit in der Informationstechnik (BSI)

Als zusätzliche weitere Behörde steht das BSI als bundesweit tätige, unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit zur Verfügung. Es schützt nicht nur die Netze des Bundes, sondern unterstützt auch gewerbliche und private Anbieter sowie Nutzer von Informationstechnik. Ein besonderes Augenmerk liegt auf dem Schutz Kritischer Infrastrukturen nach dem 2015 verabschiedeten IT-Sicherheitsgesetz, weshalb dem BSI dortige IT-Sicherheitsvorfälle gemeldet werden müssen (s. o. 3.).

Das BSI berät bei der Findung ausgewogener Lösungsstrategien in Fragen der Informationssicherheit, koordiniert Beratungsanfragen und führt grundlegende Ausbildungen in diesem Umfeld durch. Hierzu gehören auch Online-Schulungen.

Die Sicherheitsberatung beim BSI ist zentrale Anlaufstelle für Unternehmen zur Unterstützung bei Fragen zur Informationssicherheit. Zu beachten ist aber, dass das BSI wegen der Melde- und Weitergabefunktion keine Vertraulichkeit hinsichtlich der Vorfälle in Unternehmen zusichern kann.

Cyber-Sicherheitsnetzwerk (CSN)

Seit September 2021 gibt es das beim BSI angesiedelte Cyber-Sicherheitsnetzwerk. Dies ist ein freiwilliger Zusammenschluss von qualifizierten Experten für eine Vorfallbearbeitung, die ihre individuelle Expertise zur Behebung von IT-Sicherheitsvorfällen zur Verfügung stellen. Durch die Übernahme reaktiver Tätigkeiten sollen Vorfälle erkannt und analysiert werden, um das Schadensausmaß zu begrenzen und weitere Schäden abzuwenden. Dabei erfolgt die Unterstützung vorfall- und zielgruppenspezifisch.

Das Cyber-Sicherheitsnetzwerk bildet die zentrale erste Anlaufstelle sowohl für Betroffene als auch für Experten. Die Geschäftsstelle des CSN nimmt die Registrierungen vor und beantwortet alle prozessualen und organisatorischen Fragen.

Kontakt

Die Informationssicherheitsberatung erreichen Sie unter:
Telefon: (0228) 99 9582-333
FAX: (0228) 99 109582-333
E-Mail: Sicherheitsberatung@bsi.bund.de

Weitergehende Informationen finden Sie unter:
BSI – Unternehmen (bund.de)
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/cyber-sicherheitsnetzwerk_node.html

---

4.4 Bundesamt für Verfassungsschutz (BfV)

Das BfV unterstützt Unternehmen bei der Prävention. Unter dem Stichwort Wirtschaftsschutz sollen deutsche Wirtschaftsunternehmen vor Wirtschaftsspionage, Sabotage und den damit einhergehenden Wettbewerbsnachteilen bewahrt werden. Das BfV steht den deutschen Unternehmen als Ansprechpartner für Sicherheitsfragen zur Verfügung.

Kontakt

Kontakt zum Referat für Wirtschaftsschutz im BfV:
Telefon: (0221) 792-3322
E-Mail: wirtschaftsschutz@bfv.bund.de

Weitergehende Informationen finden Sie unter:
Bundesamt für Verfassungsschutz - Wirtschafts-/ Wissenschaftsschutz

4.5 Allianz für Cyber-Sicherheit (ACS)

Außerhalb des rein behördlichen Bereichs gibt es weitere Anlaufstellen, die Unterstützung im Bereich IT-Sicherheit bieten. Die durch BSI und BITKOM initiierte Allianz für Cyber-Sicherheit hat sich das Ziel gesetzt, die Sicherheit des Standortes Deutschland zu stärken. Dazu stellt die Initiative ein umfangreiches Informationsangebot mit Empfehlungen für die Wirtschaft und andere professionelle Bedarfsträger bereit. Die ACS bietet neben dem thematisch geordneten Einstieg in die Materie weitergehende Informationen und Angebote. Unter anderem wird ein Cyber-Sicherheitscheck zum Stand der Cyber-Sicherheit im Unternehmen angeboten sowie eine Liste qualifizierter Dienstleister.

Ein weiterer wesentlicher Bestandteil der ACS ist der Erfahrungsaustausch unter den über 5.000 Teilnehmern. Registrierte Teilnehmer erhalten Zugriff auf ein erweitertes Informationsangebot, insbesondere zur Sicherheitslage durch monatliche Lageberichte, Warnmeldungen sowie weitergehenden Hintergrundinformationen. Aufgrund der teilweise vertraulichen Natur dieser Informationen muss die Weitergabe dieser Inhalte restriktiv gehandhabt werden. Die Teilnahme an der Allianz steht grundsätzlich allen Institutionen mit Standort in Deutschland offen. Die Teilnahme ist kostenlos und kann jederzeit beendet werden.

Kontakt

Die Geschäftsstelle Allianz für Cyber-Sicherheit erreichen Sie unter:
Telefon: (0800) 2741000
E-Mail: info@cyber-allianz.de

Weitergehende Informationen finden Sie unter:
ACS – Allianz für Cyber-Sicherheit – ACS (allianz-fuer-cybersicherheit.de)

4.6 Initiative Wirtschaftsschutz

Im April 2016 wurde auf Bundesebene die "Initiative Wirtschaftsschutz" als gemeinsame Einrichtung von Wirtschaft und Staat gestartet. Sie bündelt die jeweilige Expertise und hat sich zum Ziel gesetzt, zentrale Unternehmenswerte für Deutschland und seine Wirtschaft besser zu schützen. Dazu arbeiten mehrere Akteure von Wirtschaft und Staat, koordiniert vom Bundesministerium des Innern, zusammen:

- Bundesverband der Deutschen Industrie (BDI)
- Deutscher Industrie- und Handelskammertag (DIHK)
- Allianz für Sicherheit in der Wirtschaft (ASW Bundesverband)
- Bundesverband der Sicherheitswirtschaft (BDSW)
- Bundesamt für Verfassungsschutz (BfV)
- Bundeskriminalamt (BKA)
- Bundesnachrichtendienst (BND)
- Bundesamt für Sicherheit in der Informationstechnik (BSI)

Die Initiative hat u. a. ein umfassendes Schutzkonzept entwickelt, das Maßnahmen und Projekte für einen verbesserten Wirtschaftsschutz enthält.

Weitere Informationen

Weitergehende Informationen finden Sie unter:
https://www.wirtschaftsschutz.info/DE/Home/home_node.html

Hinweis

Alle Angaben dieser Publikation beziehen sich ohne jede Diskriminierungsabsicht grundsätzlich auf alle Geschlechter.