ZENTRALE ANSPRECHSTELLE CYBERCRIME

Handlungsempfehlungen für (Wirtschafts-) Organisationen

Bayerisches Landeskriminalamt

Inhalt

Handlungsempfehlungen der Zentralen Ansprechstelle Cybercrime (ZAC) in Bayern

Unsere Handlungsempfehlungen befassen sich mit der Informationstechnik (IT) als einem wichtigen Bestandteil Ihrer Unternehmenssicherheit. Basis dieser Empfehlungen sind die polizeilichen Erkenntnisse betreffend der tatsächlichen Kriminalitätslage.

Die empfohlenen Maßnahmen sind nicht als abschließend zu betrachten. Sie sollen zusammen mit unseren Vorträgen, Informationsvideos und Phänomenlagen als erster Anhalt beim Aufbau einer IT-Sicherheitsstrategie in Ihrer Organisation dienen.

Im Bereich der FAQ finden Sie zusätzlich Antworten zu häufigen Fragen.

Weiterführende Informationen erhalten Sie auch durch benachbarte Behörden (BSI, LSI, BLfV(CAZ)) und Institutionen (Bitkom, ProPK u.a.) über die Verlinkung auf unserer Webseite.

1. Organisatorische Regelungen

1.1 Beauftragung kompetenter IT-Sicherheitsverantwortlicher

Beauftragen Sie hinreichend qualifizierte Mitarbeiter mit dem Schutz Ihrer IT und/oder geeignete Dienstleister.

Elektronische Datenverarbeitung und moderne Kommunikationstechnologien sind entscheidende Erfolgsfaktoren auf den Märkten. Die systemimmanenten Angriffsvektoren können eine existenzielle Bedrohung für Ihre Organisation darstellen, insbesondere wenn die Anlagen nicht aktuell gewartet oder falsch genutzt bzw. fehlerhaft konfiguriert werden. Dabei werden die Systeme immer komplexer. Der sichere Einsatz muss zwingend von kompetenten Verantwortlichen konzeptioniert, projektiert, gewartet und ständig weiterentwickelt werden.

1.2 Verpflichtung von IT-Dienstleistern zur Unterstützung im Angriffsfall

Erheben Sie die Verfügbarkeit geeigneter Dienstleister für die Bewältigung von Sicherheitsvorfällen, zur Abwehr von Schadereignissen oder der Begrenzung von Auswirkungen durch akute Cyberangriffe. Wir empfehlen auch ohne konkreten Anlass, bereits vertragliche Vereinbarungen mit qualifizierten Anbietern zu treffen und hierbei Reaktionszeiten und Leistungsumfang festzulegen. Prüfen Sie auch, ob die Absicherung entsprechender Leistungen durch eine Versicherung sinnvoll sein könnte.

Die Abwehr von DDoS-Attacken erfordert regelmäßig die Mitwirkung des Internet Service Providers (ISP). Diese bieten für gewöhnlich auch Dienstleistungen wie DDoS-Erkennung und Mitigation an. Zusätzlich kann es erforderlich sein, bereits im Vorfeld eines Angriffs Spezialisten für die Bereinigung eines später befallenen Netzwerks oder die Wiederherstellung von Daten und Arbeitsumgebungen zu verpflichten. Auch die Täterkommunikation in Erpressungsfällen inkl. einer möglichen Zahlungsabwicklung oder die forensische Auswertung zur Identifikation des Angriffsvektors erfordert spezielles Wissen und Kompetenzen. Zu prüfen ist auch, ob eine Versicherungspolice bereits entsprechende Leistungen enthält. Jedenfalls müssen die Ansprechpartner dieser externen spezialisierten Dienstleister und Provider, der vereinbarte Leistungsumfang inkl. Vertragsnummern und Erreichbarkeit der Ansprechpartner auch analog vorhanden bzw. dem Verantwortlichen bekannt sein.

1.3 Bestandsaufnahme - Configuration Management Database (CMDB)

Erheben Sie alle Geräte und zugehörige Schnittstellen, Benutzer und deren Arbeitsbereiche sowie damit verbundene Berechtigun-

gen, installierte Programme und deren jeweiligen Stand, Daten und deren Verwendung in Ihrer Organisation.

Die gewonnene Übersicht befähigt Sie zu zielführenden unternehmerischen Entscheidungen und erhöht so mittelbar auch das Sicherheitsniveau Ihrer Organisation. Ihnen sollte jederzeit bekannt sein, welchen technischen Komponenten und Personen Sie besonders vertrauen (Trust Relationsships) bzw. ob in allen Bereichen die für den jeweiligen Prozess erforderliche Sicherheit erreicht wird.

1.4 Identifizierung und Schutz der wichtigsten Daten („Kronjuwelen“)

Definieren Sie die besonders schützenswerten Daten (Stichwort: Kronjuwelen) in Ihrer Organisation und prüfen Sie die Auswirkungen bei Nichtverfügbarkeit oder Abfluss dieser Daten. Schützen Sie diese Daten entsprechend z.B. durch Verschlüsselung oder separater Speicherung außerhalb des Netzwerks.

Schützenswert in diesem Sinne sind einerseits Daten, die Sie für Ihre Betriebsabläufe zwingend benötigen, und andererseits Daten, über die Dritte keine Kenntnis erlangen sollen (Rezepturen, Patente, Kontodaten, Einkaufspreise und -mengen, Kooperationspartner und Vertragsbedingungen usw.), insbesondere aber auch personenbezogene Daten Ihrer Mitarbeiter und Kunden.

1.5 Gefahrenanalyse und -begrenzung

Erheben Sie die möglichen Folgen von Systemausfällen und/oder dem Abfluss von Daten für die einzelnen Arbeitsbereiche Ihrer Organisation sowie die Auswirkungen über interne und externe Schnittstellen, auch auf Kooperations- bzw. Kollaborationspartner (Gefahrenanalyse). Versuchen Sie diese denkbaren Auswirkungen durch organisatorische Regelungen und technische Maßnahmen möglichst zu begrenzen.

Nur wenn Ihnen die Folgen von Systemausfällen und Datenabflüssen in den einzelnen Arbeitsbereichen bekannt sind, können Sie zielführende unternehmerische Entscheidungen treffen, um diese abzuwenden und ein angepasstes Maß an Sicherheit für den jeweiligen

Bereich zu entwickeln. Möglicherweise können Sie dadurch auch im Rahmen einer Kosten-Nutzen-Abwägung auf bestimmte Investitionen verzichten. Werden Sie Ihrer Verantwortung gerecht, schützen Sie Ihre Organisation und Ihre Partner vor nachhaltigen Schäden durch Cybercrime.

1.6 Funktionsbezogene Begrenzung der Nutzerrechte

Beschränken Sie die Nutzerrechte der Mitarbeiter auf das für die jeweilige Aufgabenerfüllung notwendige Maß. Löschen Sie Benutzer oder aktualisieren deren Rechte nach einem Aufgabenwechsel.

Es gilt, den Schaden durch ein kompromittiertes Konto und die Reichweite eines unautorisierten Zugriffs möglichst zu begrenzen. Ggf. kann es sinnvoll sein, mehrere Benutzerkonten für einen Mitarbeiter anzulegen, wenn dieser verschiedene Aufgaben wahrnimmt oder in verschiedenen Arbeitsbereichen tätig ist (z.B. mehrere Konten für einen Administrator mit unterschiedlichen Berechtigungen/Sichten).

1.7 Bereinigung alter Datenbestände

Löschen Sie nicht mehr benötigte Daten, insbesondere personenbezogene Daten. Oder verschieben Sie diese in das passende Netzsegment bei einer Umorganisation von Aufgabenbereichen.

Bei einem erfolgreichen Angriff auf Ihre Organisation können auch diese Daten abfließen und vergrößern unnötig das Ausmaß des Schadens. Die Vorgaben der DSGVO sind zwingend einzuhalten. Weiter Informationen hierzu erhalten Sie von der zuständigen Datenschutzaufsichtsbehörde.

1.8 Definition von Arbeitsprozessen, Controlling und Berechtigungen

Regeln Sie die Abläufe kritischer unternehmerischer Vorgänge z.B. im Zahlungsverkehr. Bei größeren Zahlungen empfehlen wir, die Freigabe von einem Vorgesetzten prüfen zu lassen (Controlling), und/oder die Verwendung von Zwei-Faktoren-Authentifizierungen etwa bei der Änderung von Kontoverbindungen.

Das Vier-Augen-Prinzip vermeidet Flüchtigkeitsfehler und schädliches Verhalten von Mitarbeitern. Mehrstufige Berechtigungsprüfungen erschweren es Angreifern, Zugriff auf Ihr Netzwerk zu erhalten. Sichern Sie die verschiedenen Bereiche Ihrer Organisation entsprechend der Wahrscheinlichkeit und dem potentiellen Ausmaß eines Schadens. Der zweite Faktor sollte nicht „phishable“ sein, d.h. Hardware Token oder biometrische Sicherungen über Handy sind zu bevorzugen.

1.9 Verschlüsselte Kommunikation

Verwenden Sie verschlüsselte Kommunikationsmethoden, wenn Sie nach extern kommunizieren.

Bedenken Sie, dass bei unverschlüsselter Kommunikation jederzeit Dritte Kenntnis nehmen und die erhaltenen Informationen böswillig gegen Ihre Interessen verwenden können.

1.10 Bestimmung von Verantwortlichen und Eskalationsparametern

Legen Sie Verantwortlichkeiten für die erforderlichen Maßnahmen nach IT-Sicherheitsvorfällen fest, inkl. der Parameter für die jeweilige Eskalation.

Definierte Verantwortung erhöht das Reaktionsvermögen Ihrer Organisation. Eskalationsstufen ermöglichen ressourcenschonende Abläufe bei niederschwelliger Reaktionsbereitschaft.

1.11 Entwerfen von Planentscheidungen

Treffen Sie Planentscheidungen für die mög-

lichen Szenarien und stellen diese den jeweiligen Verantwortlichen zur Verfügung. Überprüfen Sie diese regelmäßig.

Die Frage ist nicht ob, sondern wann Ihre Organisation von einem Sicherheitsvorfall betroffen ist. Eine gute Vorbereitung der Organisation und Vernetzung der Verantwortlichen lässt Sie schnell und zielführend reagieren und vermindert zudem evtl. Fehler bei der Bewältigung.

1.12 Entwicklung von Notfallkonzepten und Wiederanlaufplänen

Entwickeln Sie ein Notfallkonzept und Wiederanlaufpläne nach einem teilweisen oder vollständigen Systemausfall. Nehmen Sie auch eine Risikobewertung und Kostenschätzung für den Fall der Umsetzung des Notfallkonzepts vor.

Die Evolution der kriminellen Strukturen und deren Fähigkeiten machen einen zukünftigen Schadenseintritt durch Cybercrime zu einem zunehmend wahrscheinlichen Ereignis. Eine gute Vorbereitung ermöglicht eine Verkürzung der Chaosphase nach einem Angriff und reduziert das Ausmaß des Schadenseintritts.

1.13 Einsatzbereite Arbeitsmittel (Menge, Ort, Zeit, Qualität, Aktualität)

Stellen Sie sicher, dass die erforderlichen Arbeitsmittel für die Bewältigung eines Sicherheitsvorfalls ausreichend vorhanden und an der richtigen Stelle verfügbar sind.

Resultierend aus o.g. Notfallkonzepten und Planentscheidungen werden Maßnahmen und vorzunehmende Handlungsschritte definiert, deren Umsetzung ggf. an bestimmte Materialen und Informationen gebunden ist (z.B. Lieferlisten, Warenbestand, Vertragsdaten für IT-Dienstleister, Ansprechpartner und Erreichbarkeit, Speichermedien, Kabel für die Verbindung bestimmter Schnittstellen u.a.).

1.14 Schaffung von Rückfallebenen

Schaffen Sie Rückfallebenen für kurz-, mittel- und langfristige Systemausfälle.

Über welchen Zeitraum kann Ihre Organisation ohne den Einsatz Ihrer IT (inkl. Kommunikationsmedien) die Arbeit fortführen? Die einzelnen Arbeitsbereiche sollten in die Lage versetzt werden, ihren Aufgaben auch mit analogen Mitteln nachzukommen, oder es sollten zumindest nicht vernetzte Arbeitsmittel vorrätig und einsatzbereit sein.

1.15 Verwendung sicherer Passwörter

Wählen Sie für jeden Dienst unterschiedliche und sichere Passwörter. Ändern Sie diese in jedem Fall bei der ersten Inbetriebnahme einer Komponente ab.

Default Einstellungen führen immer wieder zu vermeidbaren Sicherheitslücken. Passwörter sollten hinreichend komplex und ausreichend lang aufgebaut werden.

1.16 Regelungen für den Einsatz privater Geräte (BYOD)

Legen Sie fest, ob Mitarbeiter Daten Ihrer Organisation auf privaten Geräten verwenden oder sich darüber mit dem Firmennetzwerk verbinden dürfen. Stellen Sie sicher, dass alle verwendeten Geräte den erforderlichen Sicherheitsstandard aufweisen.

Privat administrierte Geräte weisen in der Regel einen geringeren Sicherheitsstandard auf als professionell gewartete und aktuell gehaltene Arbeitsumgebungen. Angriffe auf sie können nicht nur zum Verlust von Unternehmensdaten führen, sondern auch über vorhandene Schnittstellen die Sicherheit des Unternehmensnetzwerks oder der Abläufe in Ihrer Organisation gefährden. Andererseits fördern private Geräte die Identifikation der Mitarbeiter mit der Organisation und die Akzeptanz der erforderlichen Sicherheitsmaßnahmen.

2. Technische Maßnahmen

2.1 Maßnahmen zur Identifizierung und Eindämmung von Schadcode

Verwenden Sie immer aktuelle Antiviren-Software und Firewalls.

So verhindern Sie zumindest, dass Angreifer bereits bekannte Sicherheitslücken ausnutzen und in Ihr System gelangen können. Erkannter Schadcode kann meist in Quarantäne genommen, sicher gelöscht und unschädlich gemacht werden. Entsprechende Komponenten sind also unverzichtbar, auch wenn Zero-Day-Exploits, Supply Chain-Angriffe, APT und andere besondere Angriffsformen Ihre Maßnahmen möglicherweise umgehen. Ein gezieltes Monitoring der laufenden Prozesse und des Netzwerkverkehrs kann durch heuristische Methoden auch zur Erkennung bislang unbekannter Schadcodevarianten führen.

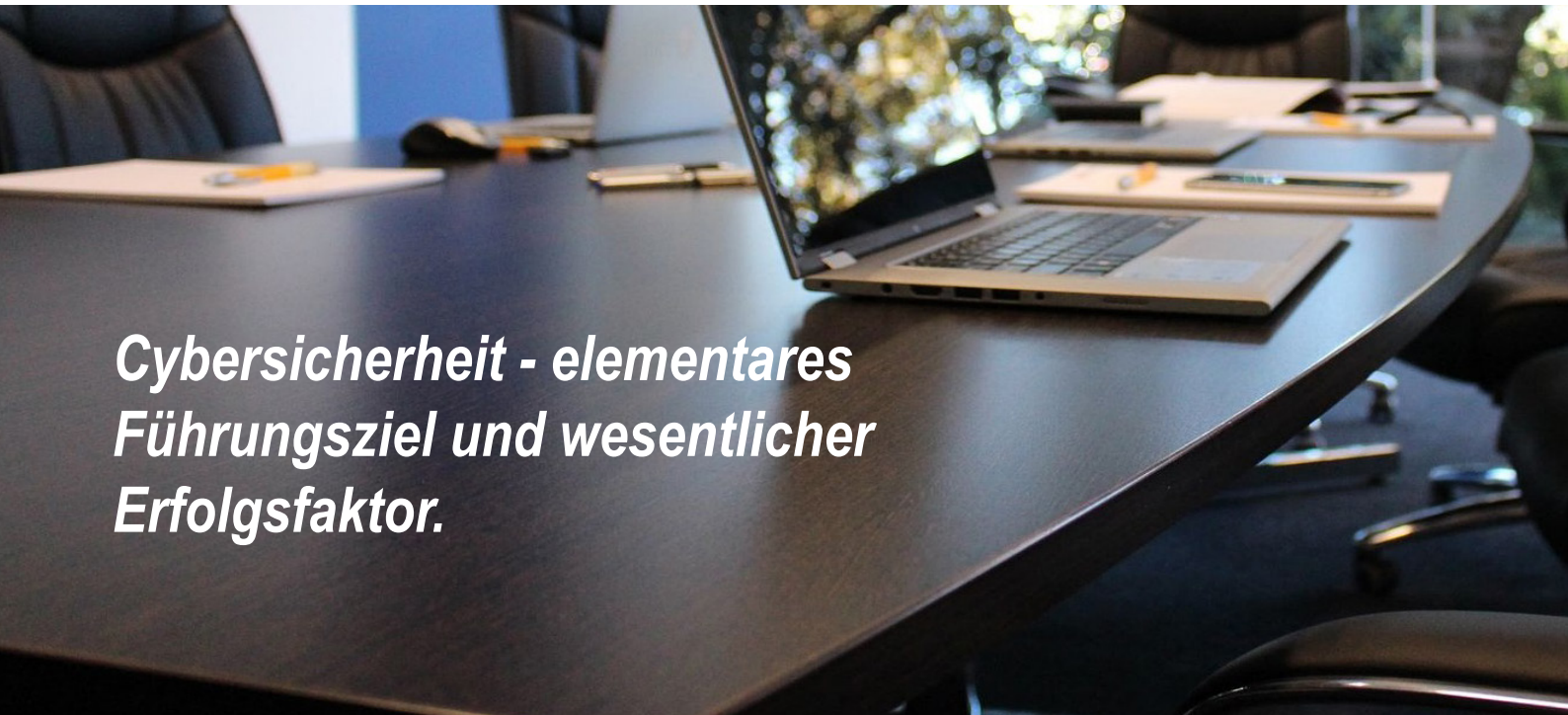
2.2 Ausreichendes Logging und Monitoring

Entwickeln Sie eine zielführende Logging Strategie und veranlassen Sie ein Monitoring aller Netzkomponenten (welche Geräte, welche Version u.a.) und Ihres Kommunikationsverhaltens. Antivirenlogs sind eine wertvolle Quelle für die forensische Aufarbeitung eines Sicherheitsvorfalls und ermöglichen ggf. die Identifikation eines Angriffsvektors. Schöpfen Sie die Möglichkeiten der Protokollierung des Verhaltens von Skripten und Programmen voll aus und halten Sie diese Daten auf vom Netzwerk getrennten Systemen vor. Kommunizieren Geräte grundlos miteinander, kann das auf ein kompromittiertes Netzwerk hinweisen. Freigegebene (kritische) Ports und Protokolle sollten im gesamten Netzwerk fortlaufend überwacht werden.

2.3 Schnellstmögliches Einspielen von Updates

Aktualisieren Sie fortlaufend alle verwendeten Programme. Patchen Sie bekannt gewordene Sicherheitslücken.

Jedes verwendete Programm kann potentiell Schwachstellen enthalten, die von Herstellern nach Bekanntwerden behoben werden. Die von den Herstellern zur Verfügung gestellten Updates und Patches müssen von den Verantwortlichen immer zeitnah eingespielt werden. Nicht mehr unterstützte Hard- und Softwarekomponenten sollten Sie entfernen.



2.4 Entschlackung der Geräte- und Programmlandschaft

Entfernen Sie Komponenten (Hard- und Software), die in Ihrer Organisation aktuell nicht benötigt werden, aus dem Netzwerk. Das gilt auch für Zugänge bei oder für andere Organisationen, sobald diese nicht mehr benötigt werden (Schnittstellen, VPN, Accounts).

Komponenten, die nicht mehr verwendet werden, sind oftmals nicht mehr im Fokus der IT-Verantwortlichen und geraten gerne in Vergessenheit. Mangels aktueller Updates und Patches können dann auch bereits veröffentlichte Schwachstellen genutzt werden und als Angriffsvektor dienen.

2.5 Etablierung einer zielführenden Backupstrategie

Entwickeln Sie eine sinnvolle Backupstrategie für alle denkbaren Schadensereignisse. Prüfen Sie, auch im Rahmen regelmäßiger Übungen (3.1), ob Ihre Systeme und Datenbestände durch vorhandene Backups tatsächlich wieder hergestellt werden können. Stellen Sie sicher, dass zumindest ein Backup für jeden Arbeitsbereich im Rahmen eines entsprechenden Angriffs nicht ebenfalls kompromittiert werden kann (vom Netzwerk und örtlich getrennt).

Backups steigern nicht nur die Resilienz gegen Cyberangriffe, auch technische Fehlfunktionen oder menschliches Handeln kann zu Datenverlusten führen. Insbesondere Ransomware-Angriffe zielen oft explizit auch auf Backups. Zu bedenken ist, dass auch ein integres Backup Datenverluste in der Regel nicht vollständig verhindern kann und dass es längere Zeit dauert, bis das neue System zu Verfügung steht. Bei einem kompromittierten System muss man dieses regelmäßig neu aufsetzen und die Daten aus dem Backup bereinigen, bevor sie eingespielt werden. Moderne Schadcodevarianten sind oft schon lange in einem befallenen Netzwerk vorhanden, bevor ein schädliches Verhalten (z.B. Verschlüsselung) ausgeführt wird. Schadcode kann also auch auf bestehenden Backups bereits vorhanden sein, lange bevor offensichtlich schädliche Funktionen (Verschlüsselung, Datenabfluss usw.) ausgeführt werden.

2.6 Entnetzung betriebswichtiger Geräte / Bereiche

Trennen Sie die Vernetzung von Komponenten, wo dies möglich und sinnvoll ist.

Prüfen Sie, ob einzelne Geräte wirklich an Ihr Netzwerk angeschlossen werden oder über das Internet erreichbar sein müssen. Die Möglichkeiten der Fernwartung stellen potentiell auch ein Risiko für die Betriebssicherheit dar, z.B. durch Cyberangriffe.

2.7 Segmentierung der Netzwerke

Veranlassen Sie eine funktionsbezogene Segmentierung der IT-Netzwerke Ihrer Organisation. Trennen Sie ggf. den Bereich Internet von der übrigen IT-Infrastruktur oder ergreifen Sie technische Maßnahmen zur Absicherung (z.B. Browser in virtualisiert gekapselter Umgebung).

Verhindern Sie, dass Schadcode bereichsübergreifend ausgeführt wird, und schützen so benachbarte Arbeitsbereiche Ihrer Organisation. Insbesondere der Datenverkehr über das Internet stellt immer wieder eine erhebliche Gefahr für Ihr Netzwerk dar und muss besonders abgesichert werden.

2.8 Abschottung von Kommunikationsmedien

Implementieren Sie Sicherheitsvorkehrungen für die Bearbeitung von Datenaustauschformaten wie E-Mail oder deren Datei-Anhänge. Abhängig von ihrer Organisationsstruktur kann die Verwendung von abgekapselten Bereichen (Sandbox) für die Ausführung solcher Pro-

gramme und die Bearbeitung potentiell inkriminierter Daten einen wirkungsvollen Schutz der übrigen Ressourcen Ihrer Organisation bieten. Für kleine Organisationen ist es oft die kostengünstigere Option, E-Mails auf einem Stand-Alone-PC zu öffnen, zu filtern und nur geprüfte Inhalte in das Firmennetzwerk zu überspielen. Gleiches gilt auch für FTP, Datenträger oder Clouddienste.

Durch die abgesicherte Ausführung von übermittelten Programmen kann deren Verhalten durch heuristische Methoden analysiert und eine Bedrohung erkannt werden. Folgeangriffe richten sich dann auf den Bereich der Sandbox und nicht gegen die Infrastruktur der Organisation. Moderne Malware-Varianten können virtualisierte Umgebungen erkennen und brechen evtl. Angriffe ab (Evasion-Techniques). Qualifizierte Dienstanbieter arbeiten deshalb mit Kaskaden von virtualisierten und physikalischen Umgebungen und ergänzen ihr Angebot durch zusätzliche Komponenten (Content Disarm and Reconstruction (CDR), intelligente Inhaltsfilter, URL-Umschreibung, verzögerte Zustellung u.a.).

2.9 Überprüfung der E-Maileinstellungen (Signaturen)

Konfigurieren Sie Ihre Kommunikationsmedien (E-Mail u.a.) sicher. Verifizieren Sie, dass Sie mit dem beabsichtigten Teilnehmer kommunizieren.

Eine digitale Signatur schützt Ihre E-Mail-Kommunikation vor der Manipulation durch Dritte. Stellen Sie sicher, dass die Konfiguration Ihres E-Mail-Servers ein Spoofing Ihrer E-Mail-Adressen verhindert. Prüfen Sie die Header-Daten der eingehenden, unsignierten E-Mails gründlich, um sicherzustellen, dass Sie mit dem beabsichtigten Teilnehmer kommunizieren.

2.10 Begrenzte Verwendung notwendiger Makros in Office-Anwendungen

Begrenzen Sie die Möglichkeit der Ausführung von Makros für Office-Produkte auf das notwendige Maß. Nutzen Sie die Möglichkeit der Signierung von Makros.

In Arbeitsbereichen, wo deren Verwendung erforderlich ist, sollten die Mitarbeiter entsprechend geschult werden. Dort, wo sie entbehrlich sind, sollten Sie aufgrund der möglichen Risiken die Verwendung blockieren auch wenn aufgrund von Sicherheitslücken die lokale Codeausführung so u.U. nicht sicher verhindert werden kann. Jedenfalls sollten Sie sicherstellen, dass nur zuvor geprüfte Makros verwendet werden.

2.11 Zugangskontrolle im Betrieb

Stellen Sie sicher, dass nur Berechtigte physischen Zugang zu Ihren Netzwerkkomponenten, Datenträgern und IT-Geräten erhalten. Kontrollieren und dokumentieren Sie diese Zugangsmöglichkeiten.

Eine Zugangskontrolle verhindert, dass Dritte Veränderungen an Ihrem System vornehmen oder auf die Inhalte zugreifen können. Auch werden einen Angriff begleitende oder vorbereitende Maßnahmen der Täter etwa durch die Verwendung von Keyloggern, Kameras oder Wanzen erschwert.

2.12 Einrichtung von Portsperren

Schließen Sie alle nicht benötigten Ports innerhalb Ihres Netzwerks und am Übergang zum Internet (Perimeter).

Beschränken Sie die notwendigen Verbindungen in Ihrem Netzwerk auf die von Ihren Netzwerkkomponenten und Programmen benötigten Kanäle. Nicht benötigte offene Ports stellen vermeidbare zusätzliche Risiken durch potentielle Angriffsvektoren dar.

2.13 Restriktive Hardwarefreigaben

Beschränken Sie den Zugang zum Firmennetzwerk auf definierte Netzwerkgeräte und Schnittstellen und erlauben Sie die Nutzung dieser Zugänge nur eingewiesenen Mitarbeitern entsprechend deren Aufgaben- und Arbeitsbereichen.

Es ist sicherzustellen, dass nur berechtigte und befähigte Personen Daten in Ihr Netzwerk einbringen oder entnehmen und hierfür nur definierte sowie besonders überwachte Schnittstellen nutzen.

2.14 Schutz Ihrer Geräte vor unbefugter Benutzung

Stellen Sie sicher, dass Geräte oder darauf gespeicherte Daten durch Verschlüsselung vor Zugriff durch Unberechtigte geschützt werden, auch bei Abhandenkommen.

Es muss gesichert sein, dass Unberechtigte nicht über die Geräte von Berechtigten Zugriff auf das Unternehmensnetzwerk erhalten oder Daten einsehen können.

3. Mitarbeiterschulung und -beteiligung

3.1 Transparenz und Übungen

Kommunizieren Sie regelmäßig Ihre Richtlinien an alle Mitarbeiter insbesondere an die jeweiligen Verantwortlichen und veranlassen Sie Übungen einzelner oder aller Arbeitsbereiche für Sicherheitsvorfälle durch Cybercrime.

Alle Mitarbeiter müssen handlungssicher die erarbeiteten Konzepte umsetzen können. Übungen ermöglichen zudem auch das Erkennen nicht zielführender Vorgaben.

3.2 Qualifikationsmaßnahmen für Mitarbeiter

Schulen Sie Ihre Mitarbeiter hinsichtlich der Erkennung von Angriffen und des angemessenen Umgangs mit Sicherheitsvorfällen sowie der definierten Meldewege.

Ihre Mitarbeiter können sich nur in dem Maße an der Weiterentwicklung Ihrer Organisation beteiligen, wie es ihr Wissensstand zulässt. Eine stetige Personalentwicklung und Weiterbildung fördert Ihre Unternehmenssicherheit.

3.3 Mitarbeiterbeteiligung und Unternehmenskultur

Beteiligen Sie Ihre Mitarbeiter an der Entwick-

lung der genannten Prozesse und fördern Sie eine offene und vertrauensvolle Kultur der Kommunikation.

Ihre Mitarbeiter leisten einen entscheidenden Beitrag für die Sicherheit in Ihrer Organisation. Werden hemmende oder sicherheitskritische Abläufe auf Arbeitsebene erkannt, aber nicht an die verantwortlichen Entscheider kommuniziert, bleibt diese Ressource ungenutzt. Übertriebener Autoritätsrespekt ermöglicht eine Vielzahl von Betrugsdelikten aufgrund fehlender Nachfragen.

3.4 Bereitstellung aktueller Netz- und Kommunikationspläne sowie von Anleitungen für Rückfallebenen

Erstellen Sie Netzpläne, Kommunikationspläne und Kurzanleitungen für die jeweilige Rückfallebene des Arbeitsbereichs und kommunizieren Sie Ihren Mitarbeitern, wie sie offline darauf zugreifen können.

Gehen Sie davon aus, dass nach einem umfangreichen Schadenseintritt möglicherweise längere Zeit kein Zugriff auf Ihre IT besteht. Um Ihr Unternehmen auch in diesem Falle arbeitsfähig zu halten, sind vorbereitete (und erprobte) Konzepte, Arbeitsmittel und analoge Informationsmedien erforderlich.

3.5 Achtsamer Umgang mit Verlinkungen

Öffnen Sie keinesfalls ungeprüft Links aus Ihren Kommunikationen (E-Mail u.a.) um sich bei einem Dienst einzuloggen.

Die Verwendung zugeleiteter Verlinkung birgt immer die Gefahr, auf maliziöse Bereiche geleitet zu werden und Ihr System dort zu infizieren. Zudem ist so nicht gesichert, wem man ggf. seine Daten (Zugangskennungen, persönliche Daten, Systemdaten, User Agent u.a.) überträgt.

Epilog - Lernspirale

Ziel unserer Empfehlungen ist die Unterstützung der bayerischen Wirtschaft bei der Härtung ihrer IT-Systeme gegen Cyberangriffe und der Gestaltung von Organisationsformen mit hoher Resilienz gegen Cybercrime, um hier Schadereignisse zu verhindern oder zu begrenzen.

Unternehmerische Entscheidungen zur Umsetzung der einzelnen Maßnahmen bzw. deren Umfang werden immer auch im Rahmen einer Kosten-Nutzen-Abwägung getroffen.

Systemimmanent können Sicherheitsvorfälle bei der Nutzung des Internet nicht vollständig ausgeschlossen werden. Es gilt, ein für den Bedarf der eigenen Organisation angepasstes Maß an Sicherheit zu erreichen.

Die empfohlenen Maßnahmen sollten fortlaufend im Unternehmen kommuniziert, dort auch kritisch überprüft, weiterentwickelt, geschult und eingeübt werden.

Zur Erhaltung der Wirkung müssen die etablierten Prozesse immer wieder neu an die aktuelle Kriminalitätslage (Phänomene) sowie an die rechtlichen und technischen Entwicklungen angepasst werden.

So erreichen Sie uns:

Zentrale Ansprechstelle Cybercrime
Tel.: 089 1212 3300
E-Mail: zac@polizei.bayern.de