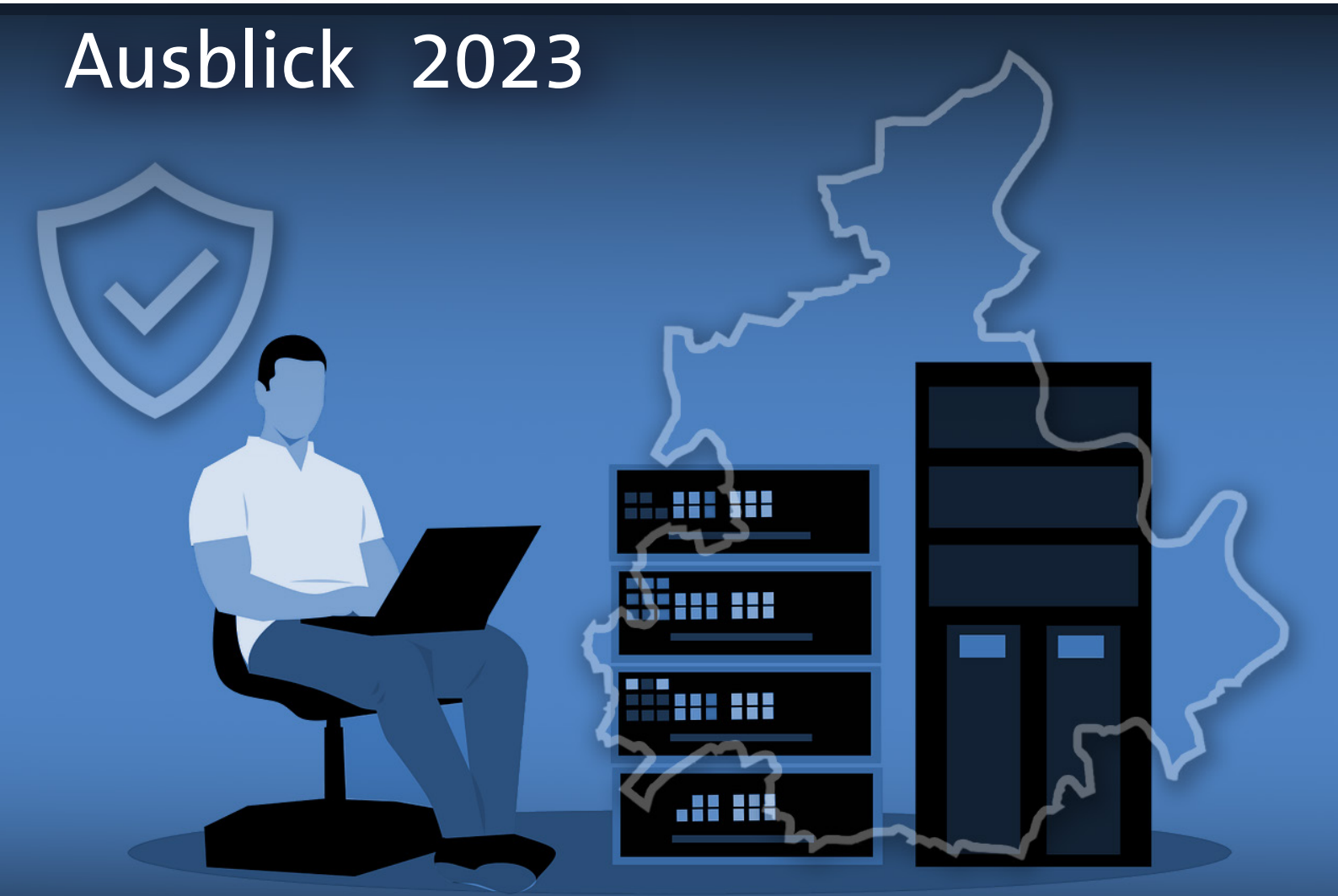
rhein kreis neuss

Jahresbericht

IT-Sicherheit

Rückblick 2022

Ausblick 2023



Vorwort

Die Schäden durch sogenannte Internet-Kriminalität sind hoch. Das BKA verweist auf Zahlen, die der Branchenverband Bitkom veröffentlicht hat. Demnach verursachte Cybercrime im vergangenen Jahr in Deutschland Schäden in Höhe von 223,5 Milliarden Euro. Einen besonders starken Anstieg gab es demnach bei sogenannten Ransomware-Attacken. Dabei verschlüsseln Kriminelle die Computer-Systeme von Privatpersonen, Behörden oder Unternehmen. Diese können dann auf ihre Daten nicht mehr zugreifen. Die Kriminellen versprechen, die Daten für ein Lösegeld wieder zugänglich zu machen.

Das Bundeskriminalamt (BKA) nennt Ransomware „die Bedrohung“ für Unternehmen und öffentliche Einrichtungen. Von Erpressungsversuchen betroffen waren u.a. die Landtage von Sachsen-Anhalt und Mecklenburg-Vorpommern, Schulen, Polizeidienststellen, Landesministerien, Universitäten und Krankenhäuser. Immer wieder trifft es zudem auch Kommunalverwaltungen.

Der kommunale Warndienst CERT NRW informiert den Rhein-Kreis Neuss täglich über bekannte Sicherheitslücken in IT-Systemen und Software. Zum Tagesgeschäft der IT gehört es deshalb zunehmend, solche Schwachstellen zu lokalisieren und abzustellen.

Mit einer weiteren organisatorischen Maßnahme soll der wachsenden Bedrohungslage in unserer IT-Sicherheitsstrategie verstärkt Rechnung getragen werden. Die Aufgaben IT-Sicherheit und die Abwehr von Cyber-Bedrohungen sollen künftig durch einen Chief Information Security Officier (CISO) inkl. Stellvertretung noch mehr Gewicht in der Kreisverwaltung erhalten. Der bisherige IT-Sicherheitsbeauftragte wird dazu aus der Abteilung ZS 4.1 - Zentrale IT herausgelöst. Zusammen mit seiner Stellvertretung, die insbesondere für die IT-Sicherheit an Kreisschulen zuständig ist, wird der CISO mit externer Unterstützung ein Information Security Management System (ISMS) aufbauen, welches hilft, die IT-Sicherheit der Kreisverwaltung nachhaltig, systematisch und workflowgestützt zu steuern, zu kontrollieren und zu verbessern.

Harald Vieten
Dezernent für IT, Digitalisierung und Bauen

Verehrte Leserinnen und Leser,

2022 haben erfolgreiche Ransomeareangriffe bei den Kommunen und zum Teil bei deren Rechenzentren erhebliche Schäden angerichtet. Besonders die kleineren kommunalen Verwaltungen sind zu einem beliebten Ziel geworden. Die IT-Verantwortlichen müssen noch intensiver als bisher vorbereitet sein, damit die Schäden an IT-Systemen durch Hacker vermieden werden. Die Verfügbarkeit und der vertrauensvolle Umgang mit den Daten müssen vor den Attacken von Cyberkriminellen effizient geschützt bleiben.

Im vorliegenden Jahresbericht werden verschiedene Teilmaßnahmen beschrieben, die alle für sich wichtige Bausteine für die gesamte IT-Sicherheitsstrategie beim Rhein-Kreis Neuss sind. Die beschriebenen Themen waren die besonderen Schwerpunkte der Verbesserungsmaßnahmen im Jahr 2022. Sie sind bei Weitem kein abschließendes Bild, welche Maßnahmen insgesamt für einen sicheren IT-Betrieb notwendig sind.

Alle IT-Sicherheitsvorkehrungen unterliegen einem wiederkehrenden Verbesserungsprozess und werden entweder durch zusätzliche technische und organisatorische Maßnahmen ergänzt oder die laufenden Prozesse werden geprüft und aktualisiert. Es gibt in der IT-Sicherheit keinen langlebigen Status Quo, durch den man beruhigt und auf Dauer abgesichert ist.

Der vorliegende Bericht soll ein Querschnitt sein, welche Projekte im letzten Jahr zum sicheren Regelbetrieb überarbeitet oder aufgrund besonderer Relevanz als Arbeitsschwerpunkte umgesetzt wurden.

Nehmen Sie bitte den ein oder anderen Hinweis auch mit, um im privaten Umfeld geschützt zu bleiben. Beachten Sie mit gesundem Misstrauen, inwieweit Sie beim digitalen Austausch Ihrer Daten und Anmeldeinformationen Dritten vertrauen können. Sie finden auf Seite 18 einige Tipps, die Sie beachten sollten, wenn Sie verdächtige Nachrichten im E-Mail Postkorb finden.

Frank Meger
IT-Sicherheitsbeauftragter

Jahresbericht zur IT-Sicherheit

Rückblick 2022 - Ausblick 2023

Inhalt

01 Die Lage der IT-Sicherheit in Deutschland

Bericht des BSI für das Jahr 2022

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Oktober 2022 seinen jährlichen Lagebericht zur Entwicklung in der IT-Sicherheit veröffentlicht. Der Bericht gibt auf über 100 Seiten einen Rückblick der letzten 12 Monate in der Cyber-Sicherheit. Zu den Bereichen Gesellschaft, Wirtschaft, Staat und Verwaltung werden die wichtigsten Erkenntnisse und Maßnahmen im Lagebericht für Deutschland zusammengefasst.

Ein besonderer Hinweis gilt der Zunahme von bekannten Schwachstellen in Hard- und Softwareprodukten. Solche potentiellen Einfallstore gefährden die Informationssicherheit. Deren Missbrauch muss durch frühzeitige Aktualisierungen vermieden werden.

Auch der russische Angrifsskrieg hat eine weitere Bedrohungslage hervorgerufen. Die Investitionen in die Cybersicherheit sollen bundes- und landesweit noch mehr verstärkt werden, wobei das BSI eine noch wichtigere Rolle als Zentralstelle spielen soll.

Die Erneuerung und der Ausbau von Netzen und IT-Systemen in der Verwaltung, die Stärkung der Sicherheitsbehörden und die Abwehrfähigkeit gegen Cyberangriffe werden als bedeutdende Ziele für mehr IT-Sicherheit in 2023 angestrebt.

Wie verletzlich die IT-Strukturen in Verwaltungen sein können zeigte im Juni 2021 der Cyberangriff auf die Verwaltungs-IT in Anhalt Bitterfeld. Die Kommune hatte nach dem Ausfall der Verwaltungssysteme den Katastrophenfall ausgerufen.

Dem aktuellen Lagebericht zufolge gelten Ransomware-Attacken nach wie vor als eine der größten Bedrohungen, zumal die kriminellen Aktivitäten sehr angespannt, dynamisch und vielfältig sind.

Laden Sie den vollständigen Lagebericht des BSI als PDF-Datei herunter:

Auszug aus dem Lagebericht des BSI

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
Identitätsdiebstahl Sextortion Fake-Shops im Internet	Ransomware Schwachstellen IT-Supply-Chain: Abhängig	Ransomware APT Schwachstellen, offene oder falsch konfigurierte Online-Server

Erster digitaler Katastrophenfall in Deutschland

207 Tage Katastrophenfall

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere bürger nahe Dienstleistungen nicht erbracht werden.

Die Anzahl der Schadprogramme steigt stetig.

Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund

116,6 Millionen zugenommen.

Hacktivismus im Kontext des russischen Krieges:

Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.

Kollateralschaden

nach Angriff auf Satelliten-kommunikation

20.174

Schwachstellen in Software-Produkten (13% davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10%** gegenüber dem Vorjahr.

69%

aller Spam-Mails im Berichtszeitraum waren Cyber-Angriffe wie z.B. Phishing-Mails und Mail-Erpressung.

90%

des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d.h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.

Geschäftsmodell Ransomware

Ransomware ist inzwischen ein gut laufendes Geschäftsmodell. Die Angreifer müssen noch nicht einmal selbst besondere IT-Kenntnisse für das Durchführen von Cyber-Angriffen haben. Kriminelle können deartige Schadsoftware inzwischen als Lizenz erwerben und damit anschließend beliebige Netzwerke angreifen.

Behörden sind weiterhin ein beliebtes Ziel für Ransomware-Angriffe. Auch wenn davon abzuraten ist, auf Lösegeldforderungen einzugehen, sind die Verwaltungen aus Sicht der Kriminellen zunächst einmal zahlungsfähige Opfer.

Für Hacker zählen Cyber-Erpressungen als lukratives Geschäft, denn die durchschnittliche Lösegeldzahlung beträgt mehr als 812.000 US-Dollar.

Backups müssen geschützt werden

Die Kriminellen greifen nicht nur den aktiv verwendeten Datenbestand an. In dem Fall könnte der Geschädigte eventuell auf eine unkompromittierte Datensicherung zurückgreifen. Vielmehr ist es das Ziel, auch die Backups der IT-Systeme und damit alle Datenversionen zu verschlüsseln. Deshalb müssen Backups als unveränderbar geschützt werden, damit die Sicherungen gegen Ransomware immunisiert sind. Man spricht von einem „immutable backup“. Hierzu gibt es verschiedene Szenarien, wie eine solche Sicherungsstrategie umgesetzt werden kann.

Der Rhein-Kreis Neuss hat in 2022 seine Backup-Strategie um zusätzliche Schutzmaßnahmen erweitert. Ein Konzept für den Betrieb eines mehrstufigen „Immutable Storage“ wurde in einem mehrwöchigen Projekt erfoglreich umgesetzt.

02 Backups vor Ransomware schützen

”Immutable Storage” wird eingeführt

Voraussetzungen für ein solides Backup

Die Möglichkeit zur Wiederherstellung von Daten erfordert sorgfältige Backups. Dabei spielt es keine Rolle, ob der Verlust auf einen Systemabsturz, eine Malware-Infektion oder einen Ransomware-Angriff zurückzuführen ist. Aus diesem Grund sollte jede IT-Organisation ein System einrichten, das eine Datenwiederherstellung sicherstellt, die vor Kompromittierung geschützt wurde.

Beim Sicherungskonzept ist maßgeblich zu beachten, dass die Konfiguration der Systeme eine eigene Verschlüsselung beinhaltet. Die Unveränderlichkeit und die physische Isolation der Backups muss durch ein angepasstes Sicherungskonzept erreicht werden. Die Backups müssen zudem auf Malware gescannt werden.

Als Ziel muss erreicht werden, eine insgesamt unveränderliche Sicherung vorzuhalten.

Neue Risiken, neue Regeln

Es gibt eine alte „3-2-1“-Regel für den Datenschutz: Bewahren Sie drei Kopien Ihrer Daten auf, eine primäre und zwei Backups. Zwei Kopien werden lokal in zwei Formaten gespeichert (z. B. Network Attached Storage, Band oder ein lokales Laufwerk), wobei eine Kopie extern in der Cloud oder einen sicheren Speicher verlagert wird.

Leider zielen laut Forbes die meisten Ransomware-Angriffe auf Sicherungssysteme ab, indem sie Endpunktdaten verschlüsseln, um eine Wiederherstellung zu verhindern. Aus diesem Grund sollte die „3-2-1-1“-Sicherungsregel eingeführt werden, wobei sich die letzte „1“ auf einen unveränderlichen Speicher bezieht.

Diese letzte „1“ lässt sich mit dem richtigen strategischen Ansatz wiederum doppelt realisieren. Beim Rhein-Kreis Neuss wurden alle notwendigen Maßnahmen dazu inzwischen ungesetzt.

3-2-1-1-0 Strategie

Die 3-2-1 Backupregel muss heutzutage durch zusätzliche Maßnahmen verbessert werden. Die Datensicherung muss auf die Unveränderbarkeit der Daten ausgerichtet werden.

3	2	1	1	0
verschiedene Kopien der Daten	verschiedene Medien	Offsite Speicherung	ist offline	Verifikation erfolgreicher Wiederherstellung

03 Benutzerkonten im Blick
durch Identitäts- und Zugriffsmanagement

Menschliche Zugriffe sind ein Risiko

Auch bei einer Kommunalverwaltung müssen heutzutage hoch komplexe IT-Umgebungen abgesichert werden. Das erfordert auch zu überlegen, welche Sicherheitsanforderungen für die IT-Systeme, die Programmoperationen, die Datenzugriffe und die zugreifenden Benutzer festzulegen sind.

In dem Zusammenhang sind trotz Endpoint-Sicherheit, Datenverschlüsselung und Firewalls gerade die Benutzerkonten ein kritisches Einfallstor. Das Aushebeln der IT-Sicherheit durch Identitätsdiebstahl stellt nach wie vor eine der größten digitalen Gefahren dar.

Benutzerdaten werden gehandelt

Personifizierte Zugangsdaten werden im Darknet als Ware gehandelt. Durch die Ransomware-Angriffe der letzten zwei Jahre und der Veröffentlichung von umfangreichen Anmeldedaten gab es einen regelrechten Boom, sodass weitere Millionen personenbezogener Datensätze angeboten wurden.

Laut Verizon Data Breach Report 2022 resultieren inzwischen 61 Prozent der Datenschutzverletzungen aus gestohlenen Anmeldedaten.

Risikofaktor externe Dienstleister und interne Administratoren

Benutzerkonten sind die bevorzugten Angriffsziele von Cyberkriminellen, um mittels Identitätsdiebstahl einen möglichst hohen Schaden anzurichten. Besonders betroffen sind häufig externe Dienstleister und interne Administratoren. Diese Personen haben oft einen privilegierten Zugang mit Zugriffen auf kritische Anwendungen und Systeme. Es gibt verschiedene Kriterien, um einen solchen Missbrauch zu verhindern. So sollten Zugangsdaten zu kritischen Systemen beispielsweise den Benutzern nicht bekannt sein. Sie sollten an einem sicheren Ort verwahrt und regelmäßig geändert werden.

Zur sicheren Authentifizierung sollte eine Multi-Faktor-Authentifizierung genutzt werden, um den Grundlevel für eine sichere Anmeldung zu erhöhen.

Mehr Sicherheit im Anmeldeprozess

Ein verbessertes Maß an Sicherheit kann auch hier erreicht werden. Dazu muss eine sichere Anmeldemethode eingesetzt werden, ohne dass es unbedingt komplizierter wird. Mittels moderner Authentifizierungsstrategien und integrierter Lösungen ist es möglich, Identitäten und Benutzerkonten besser zu schützen und noch kontrollierbarer zu machen. Dabei muss zwingend beachtet werden, dass alle ausgelagerten Anbieter über den gleichen Sicherheitslevel verfügen und nachweislich als vertrauenswürdig gelten.

Prinzip der geringsten Rechte

Die Grundannahme beim Schutz von Identitäten ist, dass Benutzer*innen, Anwendungen und Daten nicht in einer gemeinsamen vertrauenswürdigen Sicherheitszone sind. Deshalb gilt auf allen Ebenen das Prinzip der geringsten Rechte. Jede Identität soll nach erfolgreicher Authentifizierung einen genau definierten, minimalen Satz von Berechtigungen erhalten. Je nach Bedarf werden die Rechte der Identitäten entweder erweitert oder eingeschränkt. Ihnen fehlen dadurch die Möglichkeiten zu sogenannten Seitenbewegungen, die in der IT-Security besonders gefürchtet sind.

Aufbau eines Privileged-Access-Management (PAM)

Privilegierte Konten ermöglichen den Zugriff auf die sensibelsten und geschäftskritischsten Bereiche der IT der Kreisverwaltung. Ein PAM ermöglicht eine gesteuerte und protokollierte Zugriffsverwaltung von Konten und hilft damit, mehrere Angriffsvektoren auszuschalten.

Der Rhein-Kreis Neuss wird 2023 weitere Maßnahmen zur verstärkten Zugriffskontrolle umsetzen.

Architektur von Privileged Access Management für Cyber Defense

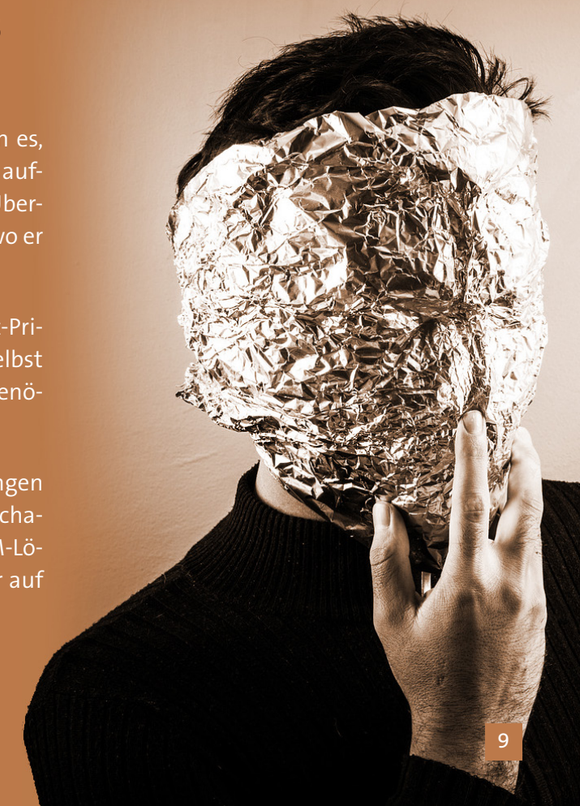
Bedingung	**Anwendungsfälle bestimmen**	**H2M:** • System Admin • Endpoint lokaler Admin • Remote Admin	**M2M:** • Konnektivität – Applikationen und Dienste • Automation – Code, DevOps, RPA	**Cloud Operations:** • Infrastruktur Berechtigungen
Orientierungsrahmen	**Anforderungen definieren**	**Kontrolle und Abdeckung** • Cyber–Sicherheitsrahmen • Plattformen & Umgebungen	**Betriebsmodell:** • User segmentation • Persistent vs. zero standing	**Bereitstellungsmodell:** • Light vs. full PAM
	Architektur entwickeln	**Kernkompetenzen:** • Governance und Verwaltung • Erkennung und Onboarding • Berechtigungsverwaltung • Sitzungsverwaltung • Erhöhungs– und Delegierungsmanagement • Protokollierung, Berichterstattung und Prüfung	**Erweiterte Fähigkeiten:** • Privilegierter Remote–Zugriff • Anwendungen und Dienste • Cloud–Infrastruktur • Privilegierte Aufgabenautomatisierung • Analytik und Reaktion • Robotische Prozessautomatisierung • Betriebstechnik	
Verfizieren	**Resilienz gewährleisten**	**Einfache Bereitstellung**	**Integration**	**Verfügbarkeit**

Wie funktioniert ein Privileged-Access Management (PAM)?

Lösungen für die privilegierte Zugriffsverwaltung ermöglichen es, Aktivitäten von Zugriffen zu überwachen, zu berichten und aufzuzeichnen. Auf diese Weise können Administratoren den Überblick über den privilegierten Zugriff behalten und feststellen, wo er möglicherweise missbraucht wird.

Die privilegierte Zugriffsverwaltung arbeitet nach dem Least-Privilege-Prinzip (Prinzip minimaler Berechtigungen), so dass selbst privilegierte Benutzer nur auf das zugreifen dürfen, was sie benötigen.

Administratoren müssen Anomalien und potenzielle Bedrohungen leicht erkennen können, wenn sie sofort Maßnahmen zur Schadensbegrenzung ergreifen sollen. Im Idealfall verfügt die PAM-Lösung über ein integriertes Warnsystem, um den Administrator auf unerwartete Aktivitäten aufmerksam zu machen.



04 Schwachstellenanalyse
erhöht die IT-Sicherheit

Irgendwo hakt es immer

Die IT-Verantwortlichen beim Rhein-Kreis Neuss kennen das: Nie ist alles auf dem aktuellsten Stand. Ob es um die Firmware-Stände von Hardware, die aktuellste Version von Gerätetreibern oder den Release-Stand der eingesetzten Software geht - bei der Vielzahl an Produkten stehen inzwischen ständig Aktualisierungsaufgaben an. Vieles davon lässt sich durch eine umfassendes Patch Management automatisiert erledigen, oft ist aber auch ein manuelles Handeln für die Umsetzung eines Updates erforderlich. Selbst die möglichen Reste einer Deinstallation von Software müssen womöglich erkannt und durch weitere Eingriffe entfernt werden.

Handlungsfeld für die IT-Sicherheit

Immer häufiger werden Updates erforderlich, um damit Sicherheitslücken zu schließen, die beim Auslassen der Aktualisierung ein Sicherheitsrisiko darstellen. Sicherheitslücken werden dann zum Beispiel zur Gefahr, wenn darüber Malware eingeführt werden kann. Die möglichen Folgen sind Datenklau, Spionage oder Erpressung durch Ransomware bis hin zum kompletten Systemausfall. Die Arbeit der Verwaltung kommt im schlimmsten Fall zum Stillstand.

Kommunaler Warndienst meldet Schwachstellen

Der Rhein-Kreis Neuss ist beim Kommunalen Warn- und Informationsdienst Nordrhein-Westfalen angeschlossen. Der Warn- und Informationsdienst des CERT NRW dient der zielgruppengerechten Aufbereitung und Weiterleitung sicherheitsrelevanter Informationen an die Kommunen in NRW.

Täglich erhält der Rhein-Kreis Neuss über einen sicheren E-Mail-Kanal Informationen zu bekannten Schwachstellen verbunden mit einer Bewertung, wie dringend eine Sicherheitslücke zu beheben ist.

Schwachstellen auffinden

Über eine Schwachstelle informiert zu sein ist die eine Seite der Medaille, aber an welchen Stellen tritt eine Schwachstelle überhaupt auf? Ein gutes Beispiel, in welchen Umfang Maßnahmen erforderlich werden, war in 2022 die „Log4j“ Sicherheitslücke. Für die weltweite IT-Security war die besondere Herausforderung, dass Log4J extrem weit verbreitet ist und sich nicht ohne Weiteres sagen ließ, ob Log4J auf den eigenen Systemen läuft. Das Open-Source-Werkzeug wird von zahlreichen weiteren Anwendungen integriert oder als Abhängigkeit genutzt. Im Internet wurde Listen mit Hiweisen gefüllt, welche Hersteller und Projekte betroffen sind. Diese Listen beinhalten mehrere hundert Einträge.

Mithilfe spezieller Scanvorgänge mussten auch beim Rhein-Kreis Neuss alle Systeme und Programme überprüft werden. Das Entfernen der Schwachstelle hatte für die IT oberste Priorität.

Schwachstellenscan automatisieren

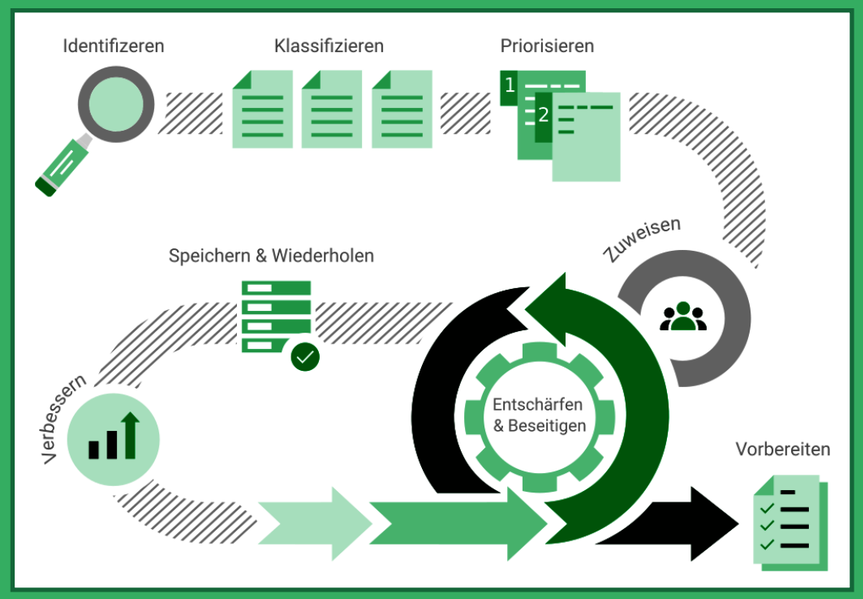
Log4j ist nur ein Beispiel einer Sicherheitslücke, auf die man umgehend reagieren musste. Datenbanken mit Schwachstellen enthalten inzwischen über 100.000 gelistete Schwachstellen verschiedenster Art. Eine kontinuierliche Analyse, ob eine Software oder ein System durch ein Sicherheitsleck angreifbar ist, wäre nicht ohne Automatisierung möglich.

Der Rhein-Kreis Neuss setzt deshalb ab 01/2023 ein „Vulnerability Management“ ein. Über einen automatisieren Prozess werden IP-Adressen mithilfe spezieller Softwaretools auf mögliche Schwachstellen untersucht - unabhängig von Software und Hersteller. Die Analyse zeigt Lücken detailliert auf und liefert Informationen zur Abhilfe. Indirekt kann der Scan beispielsweise auch zeigen, wie verantwortungsbewusst das Patch-Management umgesetzt wird. Die Ergebnisse tragen indirekt zu einem verbesserten Patch-Management bei.

Bereits wenige Tage nach der Veröffentlichung wurde die Log4Shell-Schwachstelle von Kriminellen ausgenutzt.

Kontinuierliche Sicherheit durch Scan Prozess

Von der Erkennung einer Schwachstelle bis zur Behebung und Kontrolle – neben regelmäßigen automatischen Schwachstellenscans sollte auch ein beständiger Kreislauf zur Behebung vorhanden sein. Mit der richtigen Lösung erhalten die IT Verantwortlichen anschließend eine Einstufung der Schwachstellen nach ihrem Schweregrad sowie mögliche Maßnahmen zur Behebung. Dies erlaubt eine Priorisierung und gezielte Behebung der Schwachstellen.



Quelle: Greenbone Networks

05 Managed Detection & Response

Kontinuierliche Ausfallsicherheit

Cyber-Attacken 24/7

Cyberkriminelle agieren nicht dann, wenn wir besonders aufmerksam sind, sondern rund um die Uhr. Sie können ihre Angriffe zu einer beliebigen Zeit starten und nutzen aus, dass eine durchgehende Überwachung durch das IT-Personal nur begrenzt möglich ist.

Auch wenn gute Endpoint-Detection-and-Response-Plattformen (EDR) im Einsatz sind, kann das Potenzial der bereitgestellten Analyse-Tools aus Zeit- oder Personalmangel nicht voll ausgeschöpft werden. Nach der regulären Arbeitszeit muss verstärkt auf Alarmmeldungen gesetzt werden, die wiederum eine personelle Aufmerksamkeit benötigen.

Informationsflut zu Risiken

Die IT-Verantwortlichen erhalten täglich eine Vielzahl an Warnmeldungen, die IT-Sicherheitssysteme ausgeben. Nicht alle Meldungen bedeuten dabei eine aktive Gefahr, aber die Meldungen müssen bewertet und dürfen nicht ignoriert werden. Eine schnellere Reaktion kann die Unterstützung externer Sicherheitsanalysten schaffen. Sie beteiligen sich oder übernehmen die Bewertung der Informationen und Insights von Drittanbietern und nutzen Tools zur Bedrohungsanalyse. Es gilt, aus allen sicherheitsrelevanten Hinweisen die tatsächlichen Bedrohungen durch Cyberkriminelle zu erkennen.

Managed Detection and Response (MDR) etablieren

Die Anbieter von Security-Lösungen bieten professionelle Dienste als „Managed Detection and Response Service“ an. Die Dienstleister stellen Analysten bereit, die nach möglichen Bedrohungen suchen, Warnmeldungen bewerten, individuelle Handlungsempfehlungen geben oder das Problem direkt beheben. Die notwendigen Daten liefert die EDR-Lösung (Endpoint Detection and Response). Zu einer Warnmeldung gibt EDR einen Einblick, woher die Bedrohung kam, wie sie sich ausgebreitet hat, was die Ursache war und wie groß das Ausmaß der Bedrohung ist.

Cyber-Abwehr rund um die Uhr

Die internen IT-Sicherheitskapazitäten wird der Rhein-Kreis Neuss ergänzen, indem die besonders wichtigen Aufgaben wie Erkennung, Threat Hunting und Vorfallsuntersuchungen extern unterstützt werden. Um auf angeleitete Reaktionsszenarien zurückgreifen zu können, bietet MDR einen fortschrittlichen Schutz rund um die Uhr gegen Bedrohungen, die herkömmliche Abwehrmechanismen mittlerweile umgehen können.

Der Rhein-Kreis Neuss wird eine erweiterte Sicherheitsüberwachung etablieren, bei dem ein Team von Cybersicherheitsexperten 24/7 im Einsatz ist.

EDR und MDR kombiniert einsetzen

Mit MDR können sich die firmeninternen Ressourcen gezielt auf weitere kritischen Aufgaben konzentrieren. Fortschrittliche EDR-Systeme sorgen gleichzeitig für eine merkliche Erhöhung des Durchsatzes der Analysen und reduzieren dadurch die mittlere Zeit bis zur Reaktion auf ein Minimum.

Für den Rhein-Kreis Neuss bedeutet ein MDR-Service nicht, dass man sich entspannt zurücklehnen kann. Eine verbesserte Kontrolle und Transparenz der IT-Ereignisse und die Fachexpertise von zusätzlichen IT-Sicherheitskräften sind aber eine hochwertige Ergänzung.

EDR Security Management Dashboard

Analysten erhalten über spezielle Sicherheitskonsolen einen umfassenden Überblick über die gesamte Angriffsfläche. Sobald eine verdächtige Aktivität erkannt wird , reagiert das EDR-System automatisch und/oder alarmiert einen Analysten, der den Vorfall genauer prüft.

Die EDR-Datenbank wird mit weiteren externen Datenbanken hinsichtlich Gefahrenquellen, Warnhinweisen und Schwachstellen fortlaufend kombiniert und verglichen.

Quelle: Bitdefender

06 Darknet Monitoring
deckt Datenlecks auf

Zugangsdaten zu kaufen

Hacker arbeiten hochprofessionalisiert. Es gibt darunter zum Beispiel diejenigen, die Zugangsdaten zu Netzwerken stehlen, aber nicht automatisch auch weitere Straftaten begehen. Diese Aufgabe übernehmen dann meist andere Kriminelle.

Hacker bieten stattdessen diese Datensätze im Darknet zum Verkauf an. An dieser Stelle bietet sich für die IT-Sicherheit die Chance, Schlimmeres zu verhindern. DIe IT-Administratoren können durch Darknet Monitoring, also der Analyse der Marktplätze und der hier angebotenen Datensätze, herausfinden, ob Zugangsdaten illegal veröffentlicht sind.

Analyse des Darknets zur Aufdeckung von Sicherheitslücken

Der Rhein-Kreis Neuss führt ein regelmäßiges Darknet Monitoring aus. Es ist wichtig, bekannt gewordene Passwörter und Zugangsdaten zu ändern, um möglichen Angreifern einen Schritt voraus zu sein. Dafür wird das Darknet nach festgelegten Keywords durchsucht.

Allerdings ist durch die Struktur des Darknets dessen Monitoring alles andere als einfach. Eine zentrale Suchmaschine existiert nicht, eine automatisierte Analyse ist daher unmöglich.

Monitoring as a Service

Die Abdeckung aller relevanten Quellen im Darknet ist komplex. Neben relevanten Foren und illegalen Marktplätzen sowie auf anonymen Netzwerken müssen auch Telegram-Kanäle und Chats, kriminelle Foren und Paste-Seiten im Deep Web und Open Web im Blick behalten und auf sensible Inhalte geprüft werden. Selbst über Suchmaschinen, Social-Media-Kanäle, Mobile App Stores, Code Repositories, Cloud Storage-Datenbanken oder FTP Servern finden sich Informationen, die ein Risiko darstellen.

Ein genaues Bild der Bedrohungslandschaft kann nur eine Lösung bieten, die das ganze Internet mit all seinen Quellen scannt und überwacht. Drei zentrale Schwerpunkte für das Darknet-Monitoring müssen bedacht werden:

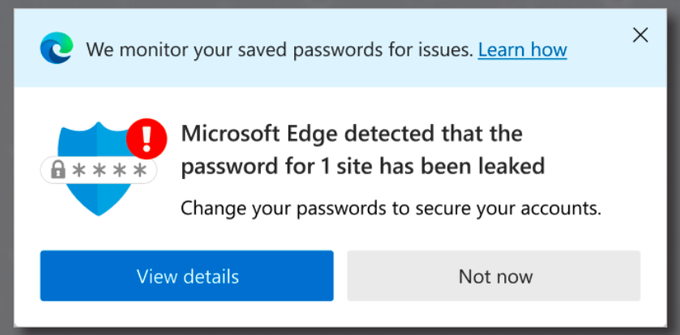
- Bedrohungen aufspüren und verfolgen
- Ungeschützte Login-Daten identifizieren
- Betrugsversuche entdecken

Für den Rhein-Kreis Neus ist auch dieser Service einer von vielen Bausteinen, der Bestandteil einer umfänglichen IT-Sicherheit ist.

Auch privat wichtig:
Anmeldedaten schützen

Moderne Browser haben Funktionen eingebaut, um bei der Verwendung von Anmeldedaten live zu prüfen, ob die eigenen Passwörter bereits im Darknet bekannt sind.

Ändern Sie bei Warnhinweisen die Passwörter, damit die Anmeldedaten nicht von anderen missbraucht werden.



Quelle: Microsoft

07 Cyber-Angriffe im Homeoffice erfolgreich abwehren

Cybergefahren am heimischen Schreibtisch

Das Arbeiten im Homeoffice klingt zunächst einmal nach einer vertrauten, sicheren Umgebung. Hier ist man jedoch in der digitalen Kommunikation den gleichen Gefahren wie in der Büroumgebung ausgesetzt. Hinzu kommt jedoch, dass man ohne den Austausch mit anderen in vielen Entscheidungen des Informationsaustauschs auf sich selbst gestellt ist.

Besondere Vorsicht bei E-Mails

Ist eine harmlos aussehende E-Mail von einer internen Firmenadresse, vielleicht verbunden mit der Bitte, sich doch für einen neuen Verteiler zu registrieren, real? Tatsächlich könnten Cyberkriminelle die Absender der Botschaft sein. Sie wollen auf diese Weise ins Verwaltungsnetzwerk einbrechen - am helllichten Tag. Solche Angriffe nennt man Phishing. Es geht in dem Fall um den Versuch, Nutzer mit gefälschten Nachrichten, Mails oder SMS auf Betrugsseiten zu locken.

Selbst für erfahrene Anwender oder sogar IT-Fachleute ist die Eindeutigkeit solcher Nachrichten nicht immer sofort erkennbar.

Zunahme von Phishing im Homeoffice

Solche Angriffe richteten sich immer öfter gezielt gegen Mitarbeiter im Homeoffice. Der Rhein-Kreis Neuss setzt deshalb im mobilen Arbeiten ausschließlich Geräte ein, die dem kontrollierten Schutz der zentralen IT (u.a. Endpoint Detection & Response, siehe Seite 12) unterliegen.

Zudem müssen die Zugriffsrechte, die Kontrolle von Programm- und Systemänderungen genauso restriktiv reglementiert sein wie bei der IT im Bürogebäude. Dazu zählt auch das Einspielen von Sicherheitsupdates unabhängig davon, an welchem Strandort ein Rechner der Kreisverwaltung verwendet wird.

Der Mensch im Mittelpunkt des Angriffs

Bei allen technischen Möglichkeiten steht bei Cyberangriffen oft die Person vor dem Rechner im Mittelpunkt einer Attacke. Phishing ist eine Form des Social Engineering, also ein Angriff auf die Schwachstelle Mensch. Technische Schutzmaßnahmen sind sinnvoll, können dies Art der Angriffe aber nicht verhindern.

Alle Beschäftigten haben eins gemeinsam: Sie sind mit der Außenwelt über E-Mail-Konten erreichbar. Das macht es den Angreifen im ersten Schritt einfach, einen Informationsaustausch zu versuchen. Während Mail-Angriffe früher noch relativ einfach zu erkennen waren, etwa durch schlechtes Deutsch im Textblock der Mail, ist das mittlerweile deutlich schwieriger. Die Nachrichten sind teilweise sehr professionell und ausführlich recherchiert, bis hin zu den E-Mail-Signaturen der vermeintlichen Absender.

Angriffe auch per Telefon

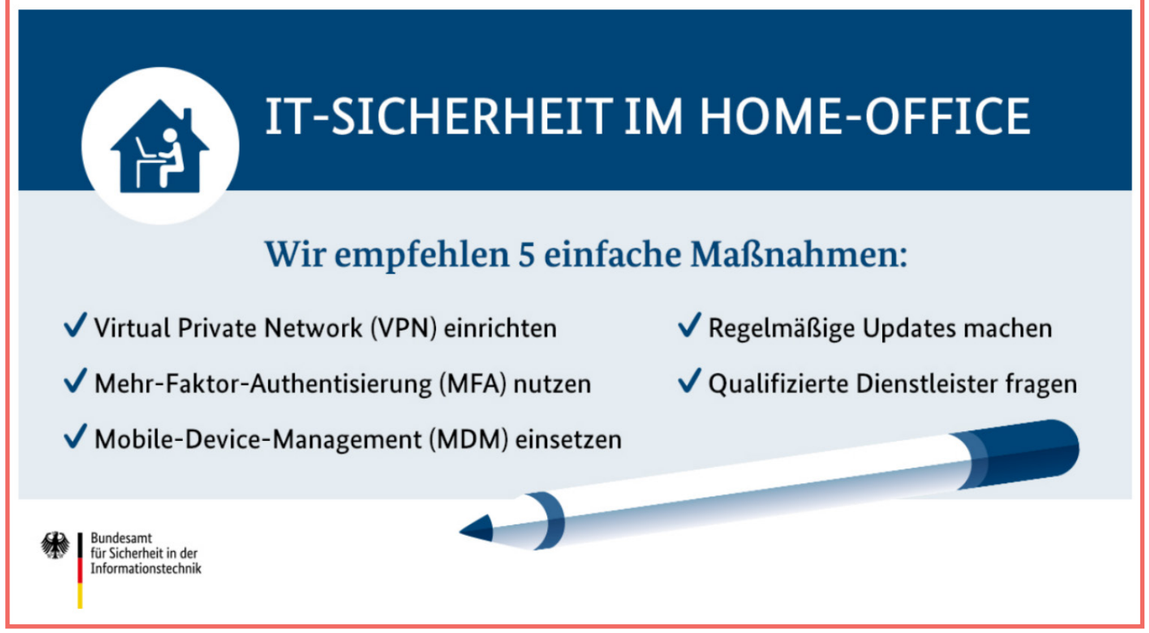
Auch per Telefon versuchen Kriminelle, sich Zugang über die Beschäftigten zu verschaffen. In dem Fall ist von „Vishing“ die Rede, einer Wortschöpfung aus „voice“ (Stimme) und „fishing“. Ein Klassiker: Betrüger geben sich am Telefon als Mitarbeitende von Microsoft aus und schaffen es, Software zur Fernwartung zu installieren. Danach haben sie die volle Kontrolle über den Rechner und einen Zugang zu den Daten.

Bei solchen Anrufen gilt der dringende Rat, sofort aufzulegen. Grundsätzlich verhalten sich die User gut geschützt, wenn sie beonders sensibel und mit einem gesunden Menschenverstand auf Cyber-Attacken und Social Engineering reagieren.

Letztlich ist ein Bündel aus verschiedenenen Sicherheitsmaßnahmen erforderlich, die der Rhein-Kreis Neuss für eine sichere, mobile Arbeitsumgebung vorgegeben hat.

Das BSI gibt Tipps für IT-Sicherheit im mobilen Arbeiten

Wir empfehlen 5 einfache Maßnahmen



Quelle: Bundesamt für Sicherheit in der Informationstechnik

08 Awareness muss trainiert sein

IT-Sicherheits-Training für alle

Der Rhein-Kreis Neuss hat 2021 mit der Einführung eines IT-Sicherheitslernprogramms für alle Beschäftigten begonnen. Seit 2022 wird das verbindliche Awareness-Lernprogramm für alle Beschäftigten in einer neuen Programmumgebung eingesetzt. Begleitet wird die Bereitstellung der Lerninhalte durch einen zertifizierten deutschen Dienstleister für IT-Sicherheitslösungen. Als Teilnehmer der Allianz für Cyber-Sicherheit befasst sich das deusche Unternehmen u.a. mit den Abwehrmaßnahmen gegen Cyberkriminalität.

Das Lernprogramm richtet sich bewusst an alle Beschäftigten. Jeder muss verstehen, welche Angriffsmethoden Hacker verwenden, um IT-Systeme und digitale Daten zu schädigen. Anstelle einmaliger Schulungen setzt man heutzutage „Security Awareness Trainings“ mit kleinen, aber häufigen Lernmodulen ein.

Vielfältige Trainings sind wichtig

Die zentrale Lernplattform bietet eine Auswahl von über 1.000 Trainingseinheiten. Aus der Lernbibliothek werden in Abständen neue Module für den Rhein-Kreis Neuss freigegeben. Zuletzt wurde speziell zu dem Thema „Social Engineering“ informiert.

Social Engineering zu verstehen ist für alle wichtig, denn viele haben bei der Arbeit einen Kontakt mit sonst unbekannten Personen. Hat darunter ein Hacker erst einmal genügend Vertrauen gewonnen, folgen E-Mails mit gefährlichen Inhalten. Die erste Hürde für eine Cyberattacke ist überwunden.

Phishing testen und melden

Alle Mitarbeiter/innen müssen lernen, die Vertraulichkeit einer Nachricht mit Links oder den Anhängen richtig einzuschätzen. Das Lernportal erzeugt deshalb bewusst falsche Phishing-Mails an alle Beschäftigte. Solche Maßnahmen werden als „Phishing Kampagne“ bezeichnet.

Wer gut aufpasst meldet die auffälligen E-Mails über einen Melde-Button im Mailpropgramm. Wichtig ist als Effekt, dass diese Maßnahme die Aufmerksamkeit für alle E-Mails hoch hält.

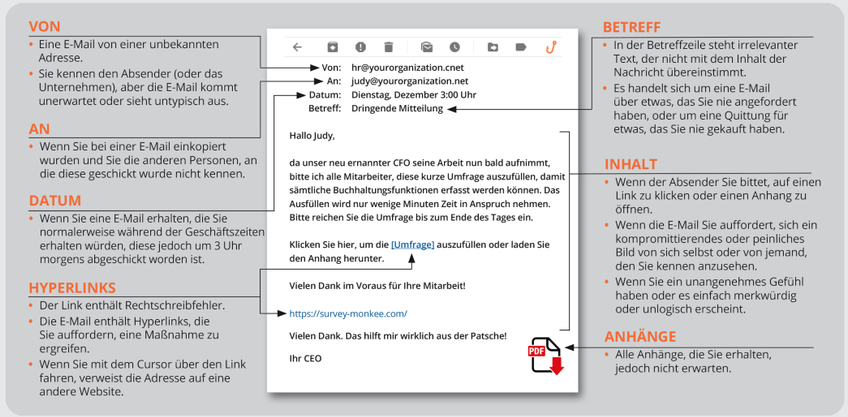
Ein Video informiert über die Meldefunktion von verdächtigen E-Mails

Eine hohe Sensibilität für den richtigen Umgang mit allen E-Mails bleibt eine ganz wichtige Herausforderung, die alle Beschäftigte betrifft und beachten müssen.

SIE sind ein Ziel!

Cyberkriminelle geben nicht auf, bevor Sie bekommen, was sie wollen. Sie wissen, dass der einfachste Zugang zur Verwaltung nicht das Hacken ist, sondern dass die User dazu gebracht werden, sie hereinzulassen. Die Mails sollten deshalb nach bestimmten Anzeichen hinterfragt werden.

Phishing ist die häufigste Form von Social Engineering. Im Folgenden sehen Sie sieben Bereiche in einer E-Mail und die entsprechenden Warnsignale.



Quelle: KnowBe4

Quelle: KnowBe4

Wachsam bleiben
Poster aus dem Security Awareness Training für den Rhein-Kreis Neuss

09 Anwendungssicherheit
auf dem Prüfstand

Bevor es an den Start geht

Für jedes neu geschaffene Programm wünscht sich die Entwicklung, dass die Anwendung den höchsten Qualitätsstandards entspricht. Durch Code-Reviews und ausführliche Tests wird weitestgehend sichergestellt, dass alles wie vorgesehen funktioniert und Fehler entdeckt werden.

Ein wichtiger Bestandteil ist dabei das Prüfen auf Sicherheitslücken. Diese Tests zu vernachlässigen kann im Nachhinein Rollbacks erfordern oder Gefahren für die Anwender und die Systeme mit sich bringen.

Schwachstellen erfordern Updates

Selbst bei best entwickelten Programmcodes werden täglich neue Schwachstellen entdeckt. Anwendungen, die bis heute noch als sicher galten, müssen bei Sicherheitsmängeln neu überarbeitet werden und erfordern neuere Programmversionen. Cyberkriminelle suchen bewusst und oft automatisiert nach solchen Sicherheitslücken.

Programmschwächen derart stellen eine unmittelbare Bedrohung dar und müssen aufgedeckt werden, bevor eine Anwendung freigegeben wird.

Angiffe der Cyberkriminellen verstehen lernen

Angreifer und Entwickler handeln grundsätzlich unterschiedlich. Entwickler haben die „Use Cases“, die Sicht eines Anwendungsszenarios, im Fokus. Angreifer hingegen denken in „Misuse Cases“. Cyberkriminelle wollen eine Anwendungslücke finden und für einen Angriff nutzen.

Oft reicht eine einzige Schwachstelle in einer Anwendung für eine Cyber-Attacke. Daher sind Tools unerlässlich, um die Sicherheit auf der Entwicklungsebene zu verbessern. Developer sollten daher selbst versuchen, mit den Werkzeugen und Techniken potenzieller Angreifer in ihre eigenen Systeme einzudringen.

Penetrationstests sind erforderlich

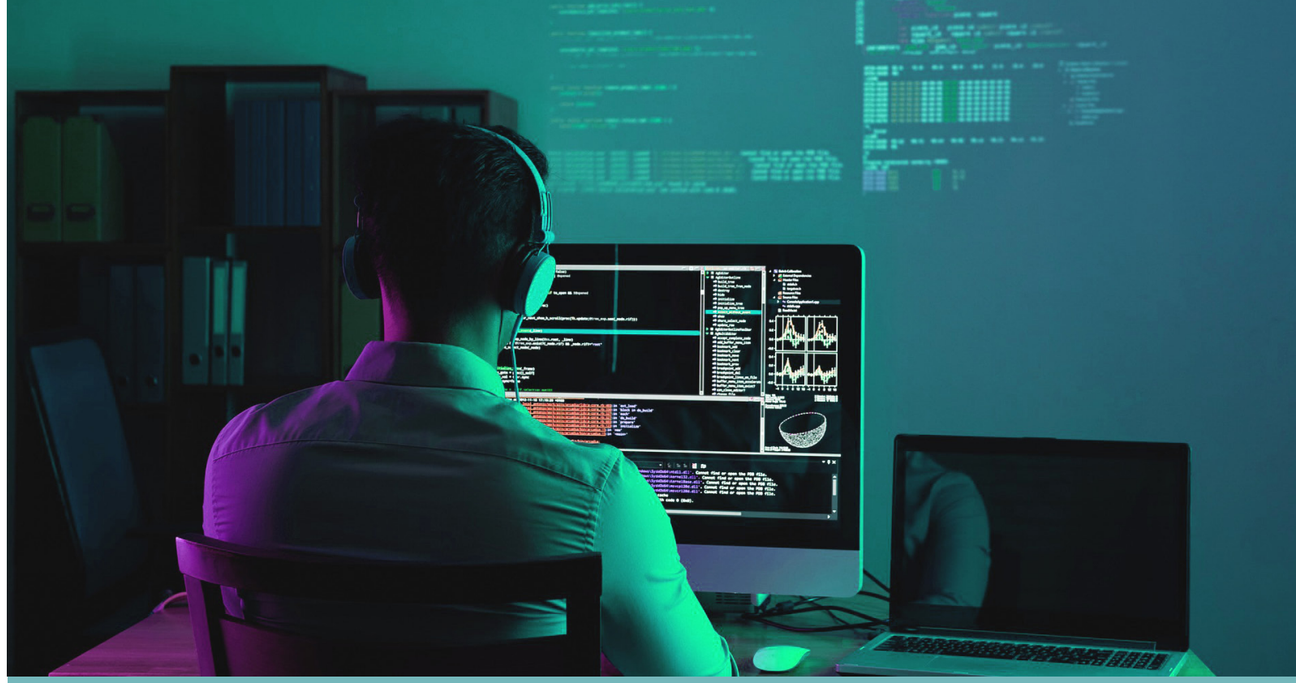
Penetrationstests sind kein Ersatz für Standardtests, Scans oder andere Überprüfungen, die zu den gängigen Sicherheitspraktiken gehören. Sie sind eine notwendige Ergänzung zu diesen Verfahren und können Schwachstellen aufzeigen, die sonst nicht in Betracht gezogen würden. Selbst ein Penetrationstests kann keine dauerhafte Sicherheit bieten. Als Momentaufnahme bestätigen sie jedoch den aktuellen Schutzzustand.

Der Versuch, in die eigenen Anwendungen mit den Tools einzubrechen, die von kriminellen Hackern eingesetzt werden, führt bei Developern zu einem erweiterten Problembewusstsein. Anstatt sich darauf zu konzentrieren, dass die beabsichtigten Verwendungen einer Anwendung möglich sind, konzentrieren sich die Entwickler zusätzlich auch auf eine unbeabsichtigte Ausführung.

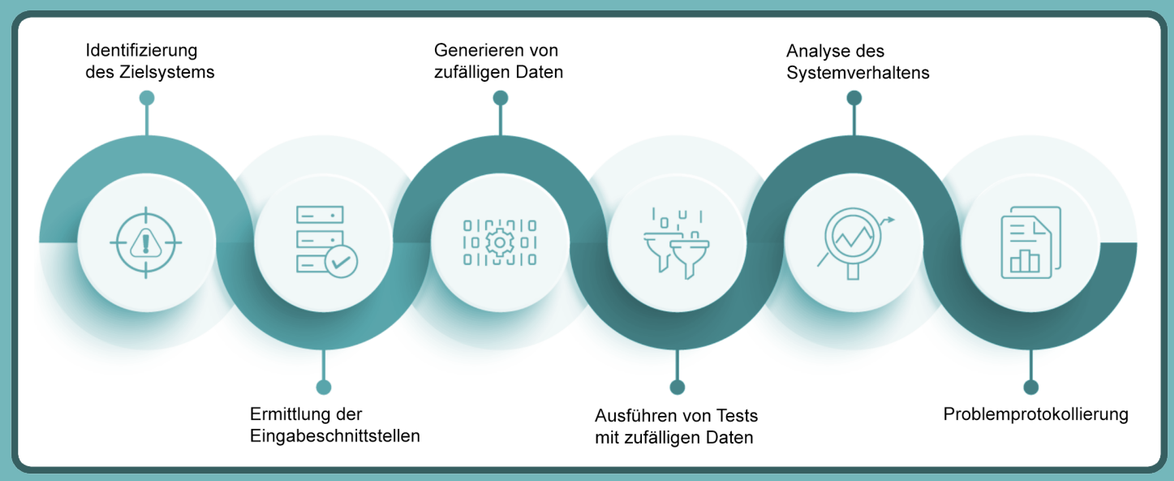
Fehler erkennen und Hacker verstehen

Sehr oft handelt es sich um Fehler im Software- Design oder in der Ablauflogik, die durch dieses Design vorgegeben werden. Der Code ist zwar entsprechend der Spezifikation geschrieben, aber durch die Definition an sich entstehen unvorhergesehene Möglichkeiten für Missbrauch und Verstöße. Diese Schwachstellen sind nicht die Schuld der Entwickler, aber sie sind mit verantwortlich für die Sicherheit der Anwendung.

Das Wissen über die Vorgehensweise von Hackern, vor allem, wenn man ihre Angriffswege und Werkzeuge selbst ausprobiert, schärft das Bewusstsein der Spezialisten für mögliche Schwachstellen in den von ihnen erstellten Codes. Je mehr Probleme bei der Entwicklung von Anwendungen bereits im Vorfeld vermieden werden, desto besser.



Praxisbeispiel
Eigener Anwendungstest mit “Fuzzing”



Quelle: FORTRA Beyond Security

Fuzzing bzw. Fuzz-Testing ist eine vom Wissenschaftler Barton Miller entwickelte Methode, um Software systematisch auf Schwachstellen zu testen. Dabei werden alle möglichen Schnittstellen der Dateneingabe automatisiert aufgerufen und mit Zufallsdaten gespeist. Dieser Prozess kann sich je nach Größe des untersuchten Software-Projekts über Stunden oder Tage hinziehen.

Ziel des Fuzz-Testing ist es, festzustellen, ob für alle möglichen Eingabevarianten die notwendigen Reaktionen im Programm hinterlegt sind. Sinnlose oder fehlerhafte Eingaben sollten möglichst durch Fehlerbehandlungsroutinen aufgefangen werden. Sind diese nämlich für bestimmte Eingaben nicht vorhanden oder funktionieren nicht richtig, kann ein Programmabsturz die Folge sein.

Dies ist eine bewährte Testmethode zum Ermitteln von Schwachstellen in Software. So werden zum Beispiel Webanwendungen per Cross-Browser-Testing auf ihre Funktionsfähigkeit in verschiedenen Webclients bzw. Browserversionen getestet.

Jahresbericht
IT-Sicherheit 2022/2023

Bildinhalte / Quellen

Bundesamt für Sicherheit
in der Informationstechnik (BSI) (S.4,5,11,17)
Bitdefender (S.12,13)
FORTRA (S.21)
Greenbone Networks (S.11)
Knowbe4 (S.18,19)
Microsoft (S.15)
Pixabay.com - CCO Lizenz (S.9,11,13,14,15,16,21W)
Rhein-Kreis Neuss (S.18)

Impressum

Rhein-Kreis Neuss
Der Landrat
Lindenstraße 2-16
41515 Grevenbroich

Frank Meger
IT-Sicherheitsbeauftragter

Telefon: 02181 - 601 1105
E-Mail: frank.meger@rhein-kreis-neuss.de