rhein kreis neuss

Jahresbericht

IT-Sicherheit

Rückblick 2021

Ausblick 2022

Vorwort

Leistungsfähige und sichere Kommunikationssysteme sind das zentrale Nervensystem unserer Gesellschaft im 21. Jahrhundert. Die IT-Sicherheit ist dabei eine wesentliche Voraussetzung für die Digitalisierung von Behörden, für die Industrie 4.0 und für den Betrieb Kritischer Infrastrukturen (KRITIS).

Das vergangene Jahr war von IT-Sicherheitsvorfällen geprägt wie nie zuvor. Über 550.000 neue Varianten von Schadstoffprogrammen an einem Tag (!) markiert einen traurigen Spitzenwert im Jahr 2021 und verdeutlicht weltweit die zunehmende Gefährdungslage durch Cyber-Kriminalität. Durch mehrstufige Angriffe ist es Cyber-Kriminellen auch bei Kommunen und Institutionen in Deutschland gelungen, Datenbestände zu verschlüsseln und damit Lösegeld einzufordern. Umso wichtiger ist es, alle rechtlichen, technischen und personellen Möglichkeiten zur Gestaltung der Digitalisierung und zur Gewährung weitreichender IT-Sicherheit permanent fortzuentwickeln.

Mit einer an die BSI-Richtlinien angelehnte Cyber-Sicherheitsstrategie setzt der Rhein-Kreis Neuss Zeichen und arbeitet daran, den zunehmenden Risiken wirksame und weitreichende Sicherheitsmaßnahmen entgegenzusetzen. Beispielhaft sei hier das neue digitale IT-Sicherheitstrainingsprogramm für die Beschäftigten erwähnt oder der für 2022 geplante Aufbau eines „Security Operation Centers (SOC)“ zur proaktiven Überwachung von Systemereignissen.

Der Blick in die Zukunft zeigt: Auf dem Erreichten dürfen wir uns nicht ausruhen. Die hohe Dynamik in der Digitalisierung und in der Cyberkriminalität andererseits wird uns auch künftig einen erheblichen, auch finanziellen, Einsatz abverlangen.

Harald Vieten
Dezernent für IT, Digitalisierung und Bauen

IT-Sicherheit ist ein Prozess. Ein Prozess, der ständig überdacht, angepasst und durch weitere Maßnahmen ergänzt werden muss. Das Jahr 2021 war deshalb stark davon geprägt, bereits vorhandene Sicherheitsstrategien zu überprüfen und zusätzliche Sicherheitsvorkehrungen einzuführen.

So wurde zum Bespiel der Viren/-Malwareschutz der Endgeräte durch eine Technologie ergänzt, die verdächtige Vorfälle der Endgeräte aufzeichnet und analysiert. Abhängig von der Bewertung eines Vorfalls können frühzeitig Reaktionen zur Abwehr der Gefahr ausgelöst werden. Was sich wie ein automatischer Schutz anhört bedeutet aber auch einen zusätzlichen Konfigurations- und Überwachungsaufwand für die IT-Verantwortlichen.

Die Mitarbeiterinnen und Mitarbeiter des Rhein-Kreises Neuss haben wir besonders stark zum Umgang mit E-Mails sensiblisiert. In dem Fall kommen moderne Lernmethoden zur Verhaltensanpassung zum Einsatz. Auch diese Maßnahme ist wichtig und wird durch die IT-Verantwortlichen aktiv begleitet.

Als letztes Beispiel, was proaktive IT-Sicherheit bedeutet, will ich die besonders häufige Reaktion auf akute Warnmeldungen zu IT-Schwachtstellen hinweisen. In einem neuen Ausmaß hat das Jahr 2021 viele Beteiligte in der IT-Abteilung einbezogen, um Sicherheitslücken entgegenzuwirken und die IT-Systeme des Rhein-Kreises Neuss zu schützen.

In 2022 sollen die notwendigen Überwachungsprozesse stärker automatisiert werden.
Hinweise dazu finden Sie im nun folgenden Bericht.

Frank Meger
IT-Sicherheitsbeauftragter

Inhalt

Die Lage der IT-Sicherheit in Deutschland

Überblick zum Bericht des BSI für das Jahr 2021

Die Cyber-Sicherheitsbehörde des Bundes veröffentlicht seinen Jahresbericht

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt in seinem jährlichen Bericht die Gefährdungslage der IT-Sicherheit in Deutschland dar. Im Jahresrückblick werden spezielle Informationen zu den Zielgruppen Gesellschaft, Wirtschaft, Staat und Verwaltung beschrieben.

Die Gefährdungslage in den Kommunen

Eine Kernaufgabe des BSI ist die Abwehr von Cyber-Angriffen auf Regierungsnetze und die Bundesverwaltung. Länder und Kommunen profitieren mit der Unterstützung des BSI bei IT-Sicherheitsvorfällen durch das CERT-Bund, durch mobile Einsatzteams und ein nationales Cyber-Abwehrzentrum.

Was Bund, Länder und Kommunen gemeinsam haben ist die drastisch gestiegene Anzahl und die Art der Angriffe mittels Schadprogrammen. Dazu zählen vor allem die starke Zunahme an infizierten Webseiten und die regelrechten Angriffswellen über E-Mails mit darin enthaltenen Links zu Schadsoftware.

Angelehnt an die Empfehlungen des BSI setzt der Rhein-Kreis Neuss auf sich gegenseitig ergänzende Vorkehrungen zum Schutz vor diesen Angriffen.

Dazu zählen unter anderem die Filterung der Webzugriffe, ein mehrstufiger E-Mail Spamschutz und das Unterbinden der Installation von Schadprogrammen.

Insbesondere auf die anhaltenden Bedrohungen durch den E-Mailverkehr hat der Rhein-Kreis Neuss zusätzliche Maßnahmen zur Sensibisierung seiner Beschäftigten umgesetzt.

Cyber-Erpressungen auch bei Kommunen

Über 550.000 neue Varianten von Schadprogrammen pro Tag waren einer der Spitzenwerte aus dem Jahr 2021. Hinzu kommt, dass die Qualität der Angriffe im zurückliegenden Jahr besonders zu genommen hat.

Durch mehrstufige Angiffe ist es Cyberkriminellen auch bei Kommunen gelungen, die Datenbestände zu verschlüsseln und damit Lösegeld einzufordern. Cyberkriminelle drohen nach dem Export der Daten mit deren Veröffentlichung und haben damit ein weiteres Druckmittel, um die Behörde zu erpressen.

Inzwischen lassen sich die Angreifer zu Gruppen zusammenfassen, die mit unterschiedlicher Schadsoftware teils im Verbund ihre Opfer angreifen.

Big Game Hunting

Hinter den Angriffen der Cyberkriminellen stecken finanzielle Interessen. Aus dem Grund konzentrieren sich die Angriffe vermehrt auf zahlungskräftige Opfer. Diese Vorgehensweise wird als „Big Game Hunting“ bezeichnet, zu Deutsch: Großwildjagd. Das Ziel ist es, möglichst hohe Lösegelder zu erpressen. Sicherheitsvorfälle dieser Art haben 2021 deutlich zugenommen.

Kommunen sollen nach den Empfehlungen des BKA und des BSI nicht auf Lösegeldforderungen eingehen. Jeder Erpressungsversuch ist zur Anzeige zu bringen und zu melden. Zudem kommt es immer wieder vor, dass Geschädigte ihre Zahlungen vergebens leisten: Die Daten bleiben trotz Lösegeldzahlung verschlüsselt.

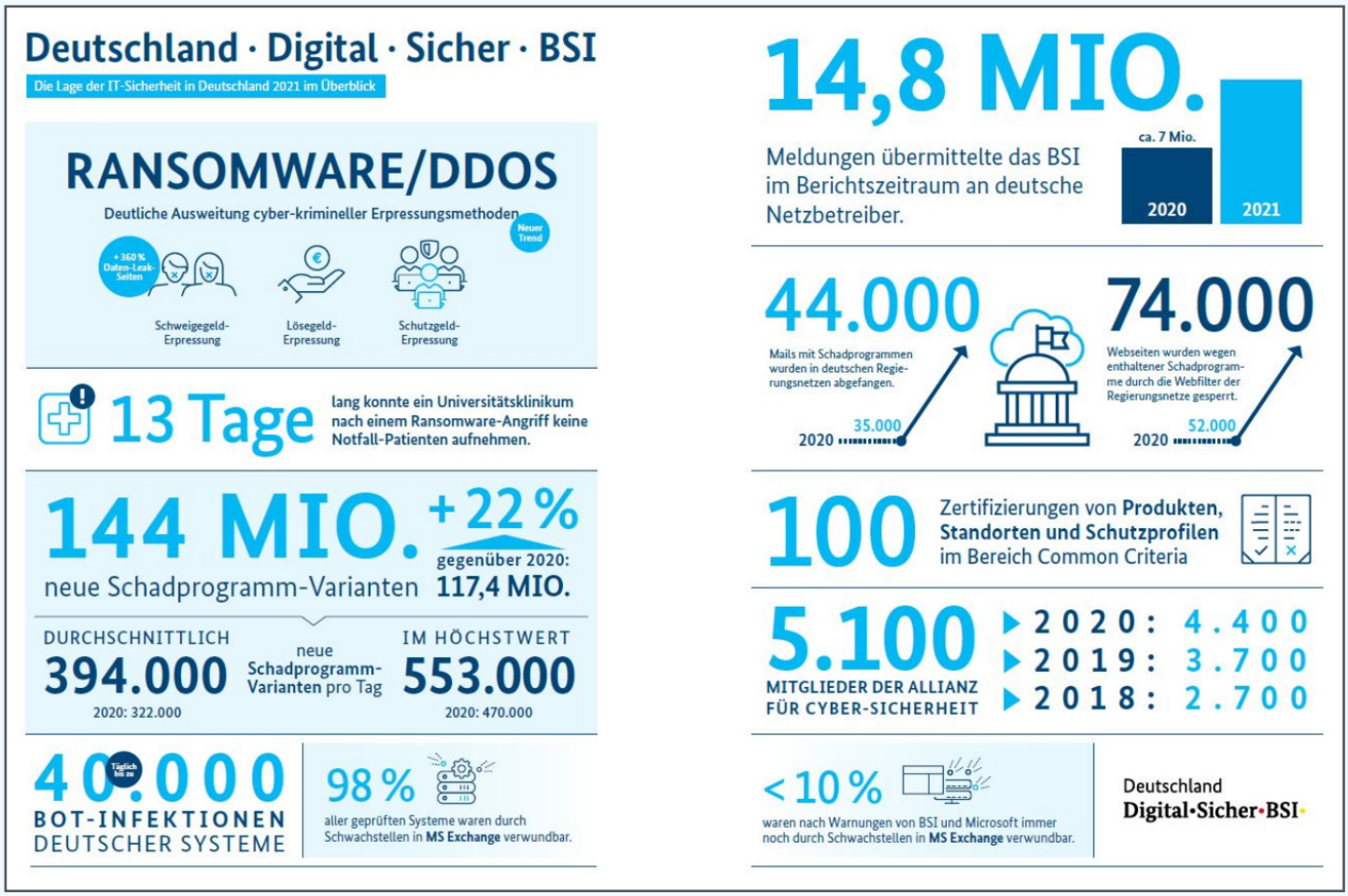
Gefährdungen durch die COVID-19-Pandemie

Das BSI registrierte bereits während des ersten Lockdowns im Frühjahr 2020 gezielte Angriffe durch Phishing- und andere Social-Engineering-Methoden.

Digitale Lösungen für das Homeoffice, abgesicherte externe Netzwerkzugriffe , Videokonferenzen etc. wurden in kürzester Zeit bereitgestellt - und damit ebenfalls das Ziel von Missbrauch und Angriffen.

Das BSI appelliert hierzu eindringlich, dass die IT-Sicherheit auch bei der Nutzung dezentraler Arbeitsweisen und bei kurzfristig bereitgestellten IT-Lösungen nicht hinten angestellt werden darf.

Quelle: BSI



Auszug aus dem Bericht des BSI zur Lage der IT-Sicherheit in Deutschland:

Höchstwerte und der zunehmende Umfang der Gefährdungspotenziale werden im Bericht dagestellt.

Laden Sie den vollständigen Bericht als PDF Datei herunter.

IT-Sicherheitsgesetz 2.0
seit Ende Mai 2021 in Kraft

Stärkung des BSI durch das IT-SiG 2.0

Mit dem IT-SiG 2.0 haben der Bundestag und der Bundesrat Maßgaben festgeschrieben, die das Bundesamt für Sicherheit in der Informationstechnik in wesentlichen Punkten deutlich stärkt. Das BSI informiert über diese wesentlichen Änderungen.

Detektion und Abwehr

Das BSI erhält verstärkte Kompetenzen bei der Detektion von Sicherheitslücken und der Abwehr von Cyber-Angriffen. Das BSI fungiert als zentrales Kompetenzzentrum der Informationssicherheit. Die sichere Digitalisierung und Mindeststandards für die Bundesbehörden können verbindlich festgelegt und effektiver kontrolliert werden.

Cyber-Sicherheit in den Mobilfunknetzen

Das Gesetz enthält eine Regelung zur Untersagung des Einsatzes kritischer Komponenten zum Schutz der öffentlichen Ordnung oder Sicherheit in Deutschland. Die Netzbetreiber müssen vorgegebene, hohe Sicherheitsanforderungen erfüllen und kritische Komponenten müssen zertifiziert werden.

So sorgt das Gesetz unter anderem für die Informationssicherheit in den 5G-Mobilfunknetzen.

Verbraucherschutz

Das BSI wird die unabhängige und neutrale Beratungsstelle für Verbraucherinnen und Verbraucher in Fragen der IT-Sicherheit auf Bundesebene. Der Verbraucherschutz ist nun eine Aufgabe des BSI. Durch die Einführung eines einheitlichen IT-Sicherheitskennzeichens für Bürgerinnen und Bürger soll in Zukunft klar erkennbar werden, welche Produkte bereits bestimmte IT-Sicherheitsstandards einhalten.

Sicherheit für Unternehmen

Der Kreis der kritischen Infrastrukturen wird um den Sektor Siedlungsabfallentsorgung erweitert. Daneben müssen künftig auch weitere Unternehmen im besonderen öffentlichen Interesse (zum Beispiel Rüstungshersteller oder Unternehmen mit besonders großer volkswirtschaftlicher Bedeutung) bestimmte IT-Sicherheitsmaßnahmen umsetzen.

Cybersicherheitszertifizierung

Das BSI ist “die Nationale Behörde für die Cybersicherheitszertifizierung”. Das BSI ist damit für die Überwachung und Durchsetzung der Vorschriften im Rahmen der europäischen Schemata für die Cybersicherheitszertifizierung zuständig. Dabei sind die Tätigkeiten Aufsichtsführung und Zertifizierung streng voneinander zu trennen und unabhängig durchzuführen.

Schutz Kritischer Infrastrukturen
durch IT-Sicherheitsgesetz und “UP KRITIS”

“... Unsere moderne Gesellschaft ist auf die Versorgung mit Strom,Wasser, Lebensmitteln und weiteren essenziellen Gütern und Dienstleistungen angewiesen. Diese werden durch Betreiber Kritischer Infrastrukturen (KRITIS) bereitgestellt.

Hierzu setzen die Betreiber hochkomplexe, stark vernetzte und von IT durchzogene Infrastrukturen ein. Um diese Infrastrukturen dauerhaft verfügbar zu halten, müssen sie adäquat geschützt werden.

Hierzu leistet die Kooperation UP KRITIS einen substanziellen Beitrag ...”

Quelle: BSI

Laden Sie die
Broschüre UP KRITIS
als PDF Datei herunter.

Cyberangriffe auf Kommunen
Deutlicher Anstieg im Jahr 2021

“Alarmstufe Rot” bei der Informationssicherheit

Mit dieser Eskalationsstufe hat das BSI in seinem Lagebericht für das Jahr 2021 die Gefahrenlage bezeichnet. Und zunehmend waren auch Kommunen davon betroffen, sodass aufgrund von Cyber-Angriffen erhebliche Einschränkungen bis zum Stillstand des IT-Betriebs von öffentlichen Einrichtungen verursacht wurden.

Aktuelle Vorfälle bei Kommunen

Wie schwerwiegend die Folgen sein können zeigen aktuelle Beispiele. Ein erfolgreicher Angriff auf einen kommunalen IT-Dienstleister in Mecklenburg-Vorpommern führte zu erheblichen IT-Ausfällen bei den angeschlossenen Kommunen des gesamten Landkreises.

Nach einem Cyber-Angriff auf die IT-Infrastruktur der Stadt Witten wurden Teile der erbeuteten Daten im Darknet veröffentlicht.

Die unmittelbaren Konsequenzen können sogar lebensbedrohlich sein. So konnte das Unversitätskilikum Düsseldorf nach einem Hackerangriff tagelang keine Notfallpatienten mehr aufnehmen. Patientendaten, Befunde und Laborergebnisse waren über Tage nicht mehr verfügbar.

Einen Zeitstrahl bekannter Schadensereignisse sehen Sie auf der folgenden Seite.

Vorbereitungen zur Handlungsfähigkeit

Auch Kommunen sollten sich auf den Ernstfall, dass deren Geschäftsprozesse ausfallen könnten, vorbereiten. Eine Analyse der wichtigste Dienste hilft, um auf ein solches Schadenseregnis bestmöglich reagieren zu können.

Das BSI hat den “BSI-Standard 200-4” entwickelt und ermöglicht dadurch einen Einstieg in das Thema “Business Continuity Management“. Dazu zählen unter anderem Dokumentenvorlagen, die an die eigenen Gegebenheiten angepasst werden können. Die Hilfsmittel werden als sogenannte „Community Drafts“ veröffentlicht, fortlaufend ergänzt und aktualisiert.

Im Ernstfall: Unterstützung durch “CERTs” und “MIRT”

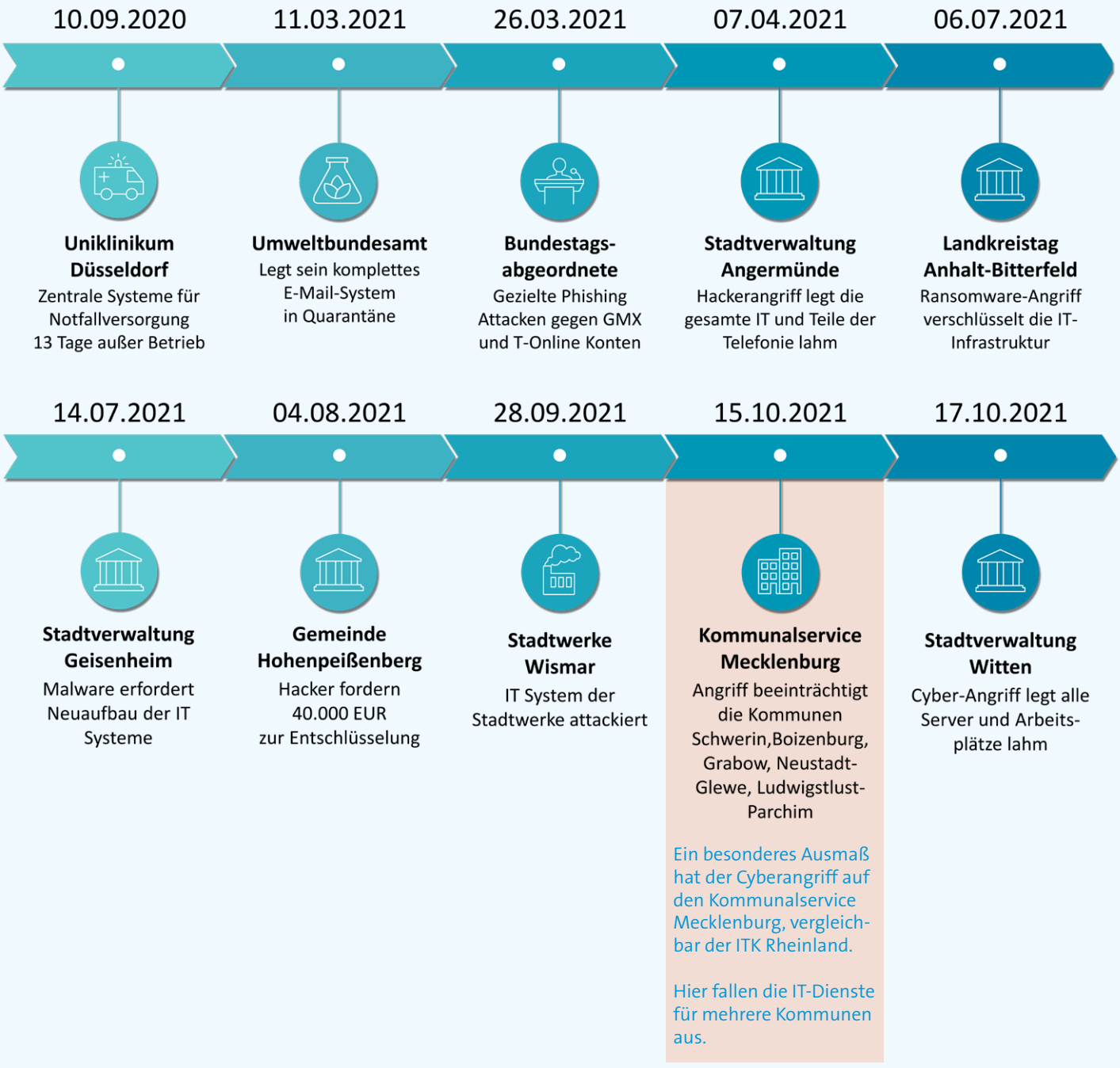
Die Länder haben Computer Emergency Response Teams (CERTs) eingerichtet, die zum Teil auch erste Ansprechpartner für die Kommunen sind. Das BSI kann auf Ersuchen der Betroffenen zusätzlich mit seinem Krisenteam, dem „Mobile Incident Response Team“ (MIRT), vor Ort unterstützen. Das MIRT ist das mobile Einsatzteam des CERT-Bund und verfügt über eine umfangreiche Ausstattung, um Betroffene vor Ort kompetent unterstützen zu können. Oberstes Ziel ist dabei zunächst, dass die betroffene Institution kritische Prozesse aufrechterhalten bzw. zeitnah wiederherstellen kann.

Rückblick auf Cyberangriffe
im Gesundheitssektor, Behörden und Kritische Infrastrukturen

2021

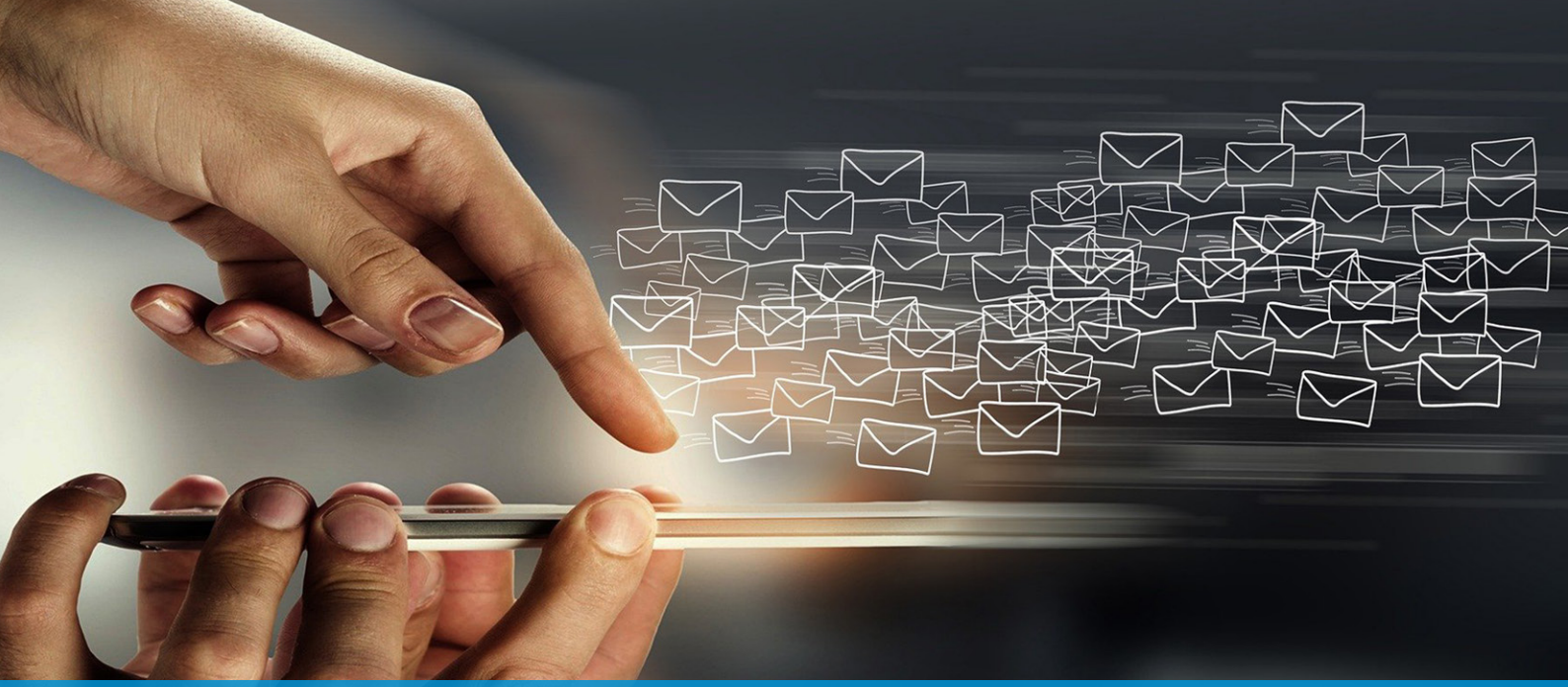
Ob Krankenhäuser, Bundesämter, Kommunen oder gezielte Personenangriffe:

Die Zahl der erfolgreichen Cyber-Angriffe hat 2021 zugenommen.



Ein besonderes Ausmaß hat der Cyberangriff auf den Kommunalservice Mecklenburg, vergleichbar der ITK Rheinland.

Hier fallen die IT-Dienste für mehrere Kommunen aus.



Cyber-Attacken via E-Mail

Phishing Kampagne erhöht die Aufmerksamkeit

Phishing Attacken gehören zum Alltag

Ein wesentlicher Teil aller Cyber-Attacken erfolgt über den E-Mail Verkehr. Die Risiken von Phishing-Attacken gehören inzwischen zum täglichen Arbeitsablauf. Insbesondere moderne, ausgeklügelte und gezielt vorbereitete Angriffe sind ohne Sachverstand kaum zu erkennen. Die notwendige Umsichtigkeit zur Verhinderung ernster Schäden lässt sich durch ein effektives Phishing-Training verbessern.

Spam Filter reichen nicht aus

Selbst eine mehrstufige und ausgereifte Spamfiltertechnik ist nicht in der Lage, alle Phishing Mails aus dem elektronischen Posteingang zu entfernen. Es bleibt ein Restanteil bei den zugestellten E-Mails und letztlich die Verantwortung und die Aufmerksamkeit jedes Einzelnen, den unseriösen Mailverkehr zu identifizieren.

Woran sind Phishing-Mails zu erkennen?

Einst waren Phishing-E-Mails unschwer zu erkennen, beispielsweise an mangelhaften Übersetzungen, schlecht gefälschten Logos und vielen Rechtschreibfehlern. Angesichts der stetig steigenden Qualität sind Phishing-Attacken mittlerweile oft nur noch an kleinen Details zu erkennen.

Feinheiten dieser Art lassen sich durch professionelle Phishing-Kampagnen erlernen. Wichtig ist hierbei, dass ein regelmäßiges Training dafür sorgt, dass das Erlernte verankert und immer wieder in das Bewusstsein der Mitarbeiterinnen und Mitarbeiter gerufen wird.

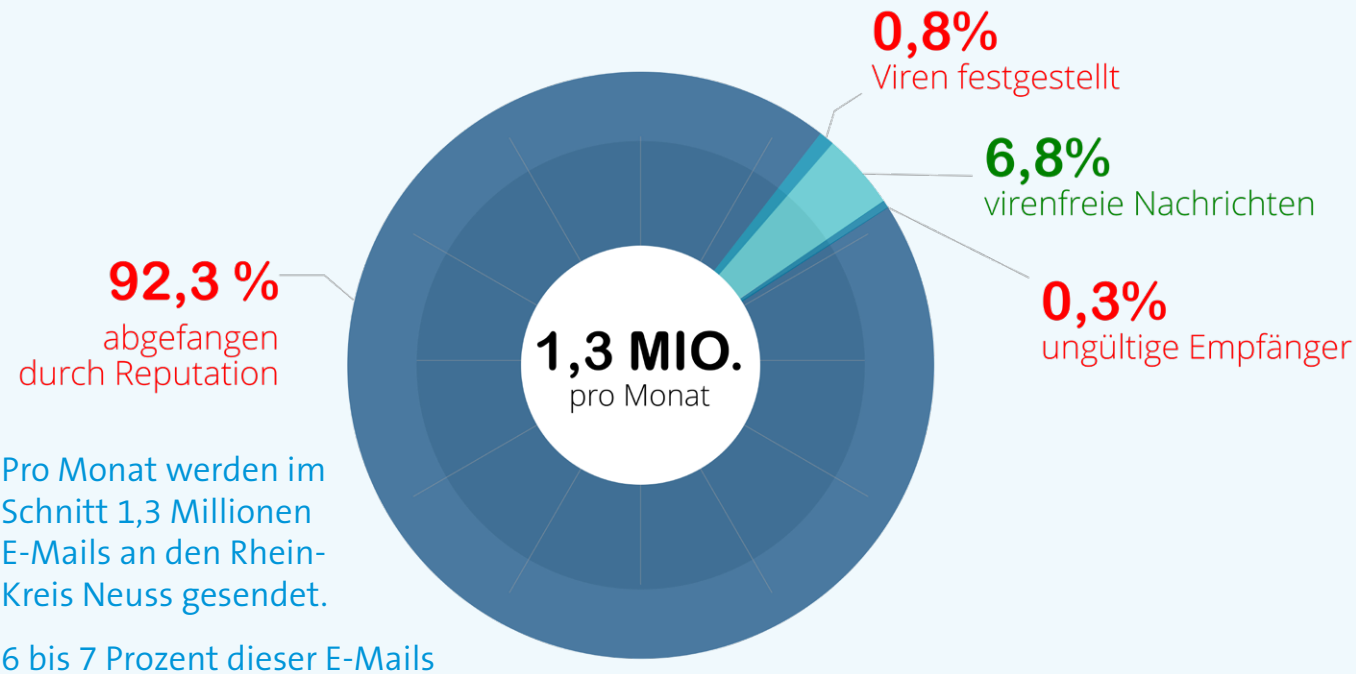
Phishing Kampagne sensibilisiert

Der Rhein-Kreis Neuss setzt das Lernmittel von Phishing Kampagnen ein. Den Beschäftigten werden automatisch und in unregelmäßigen Abständen simulierte Phishing E-Mails zugeschickt. Diese sind täuschend echt und fordern die Anwender zu einer bestimmten Aktion, etwa zum Anklicken eines Links, auf. Die Fehlerquote wird dokumentiert und in einem Report zusammengefasst. Die IT-Verantwortlichen erhalten durch anonyme Reports die Transparenz zum aktuellen “Awareness-Level” innerhalb der Belegschaft.

Die Phishing Kampagne beim Rhein-Kreis Neuss zeigt einen zunehmend vorsichtigen Umgang der Beschäftigten mit verdächtigen E-Mails.

Kommunikation mit dem IT Support

Ergänzt wird die Kampagne mit einer speziellen “Spam-Meldefunktion” im Mailprogramm. Alle Beschäftigten können mit einem Mausklick auffällige E-Mails an den IT Support melden, ohne selbst in der Nachricht zu agieren.

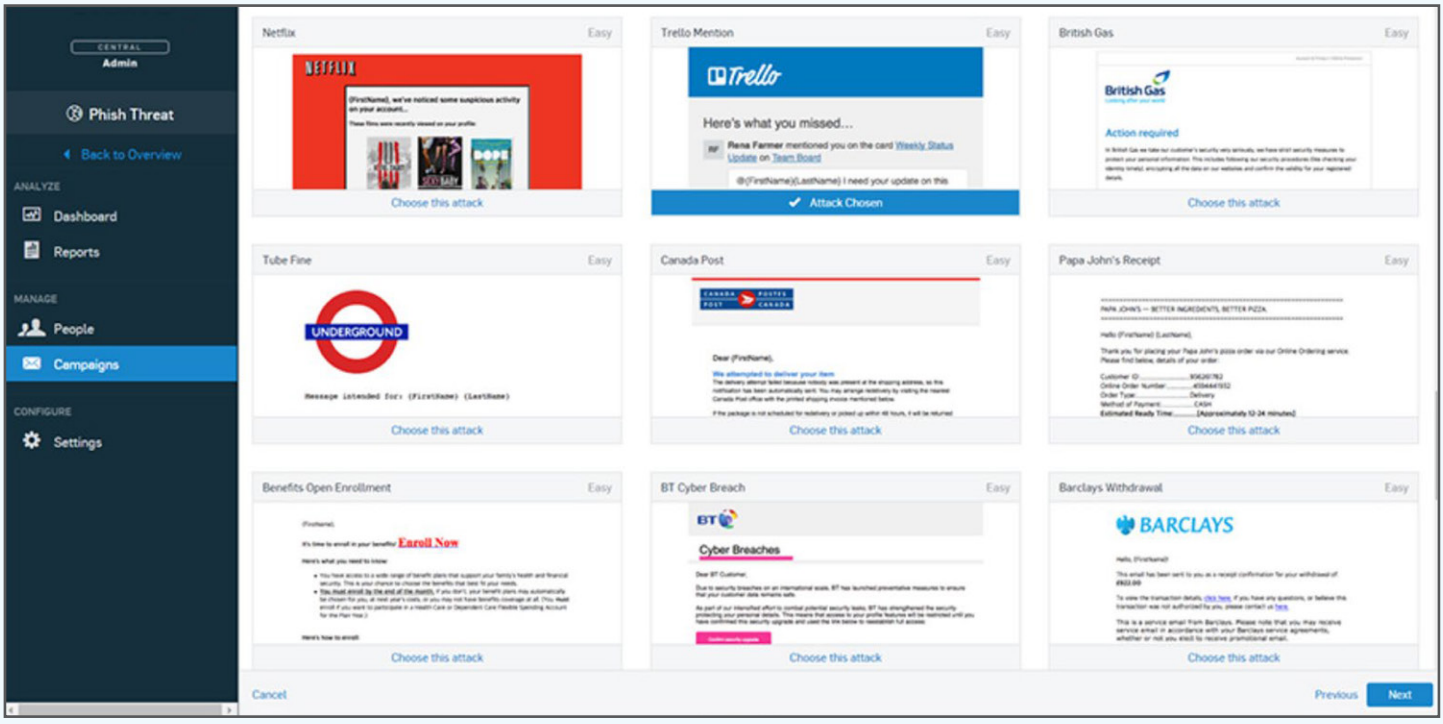


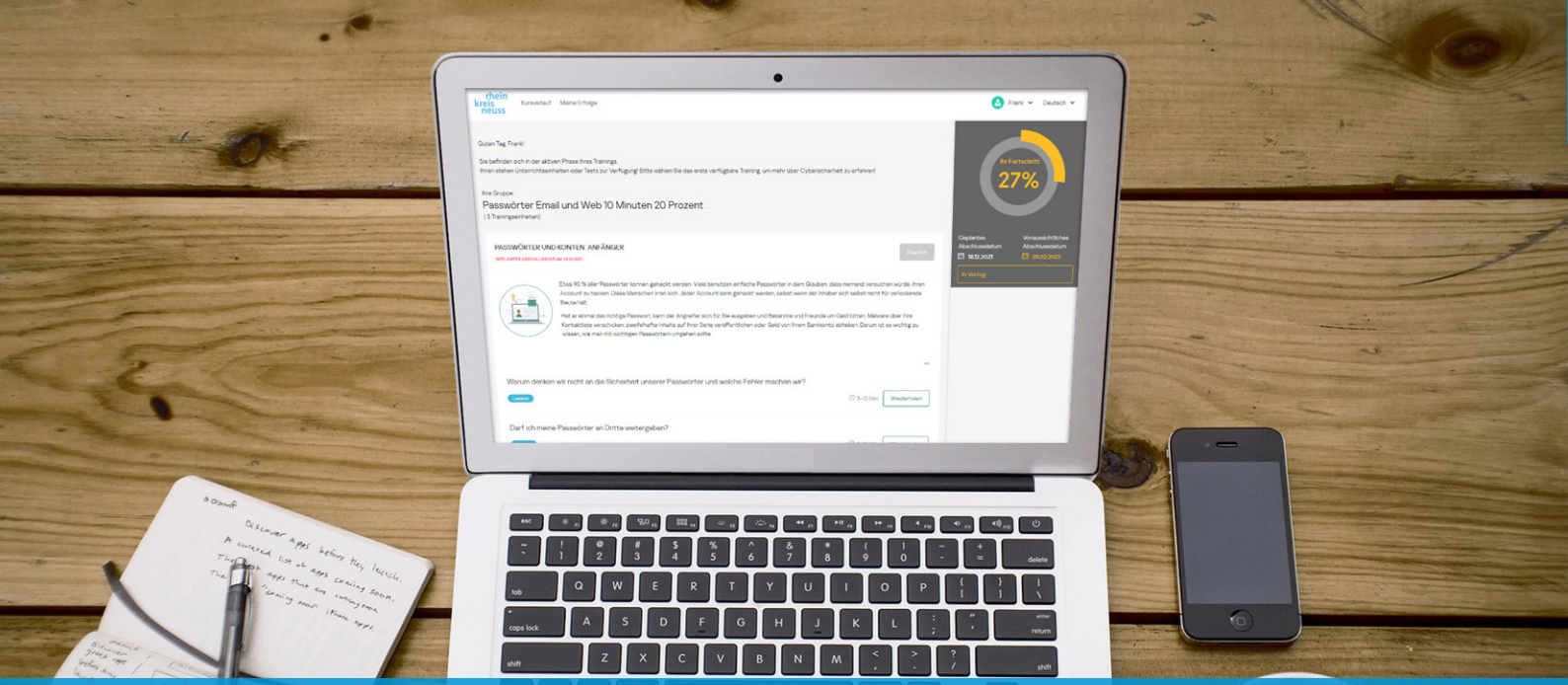
Pro Monat werden im Schnitt 1,3 Millionen E-Mails an den Rhein-Kreis Neuss gesendet.

6 bis 7 Prozent dieser E-Mails (ca.90.000) werden zugestellt. Hierin sind immer noch Phishing Mails enthalten.

Über 90% aller Angriffe auf Unternehmen beginnen mit einer Phishing-Mail.

Phishing-Simulationen sind ein erfolgreicher Bestandteil für ein kontinuierliches Awareness-Building.





Security Awareness Schulungen

Lernprogramm für alle Beschäftigten beim Rhein-Kreis Neuss

IT-Sicherheit durch eigenes Wissen

Die IT-Sicherheitsmaßnahmen alleine ermöglichen keine ausreichende IT-Sicherheit. Nur wenn die Mitarbeiterinnen und Mitarbeiter richtig reagieren und dazu geschult sind können Angriffe möglichst umfassend und erfolgreich abgewehrt werden.

Bei E-Mails oder bei Angriffen aus dem Internet sind die Benutzer oft die erste und wichtigste Verteidigungslinie. Für alle ist es wichtig, grundlegende Basiskenntnisse im Bereich der IT-Sicherheit zu erlernen. Um effektiv gegen Cyber-Angriffe auf Beschäftigte vorzugehen bedarf es eines nachhaltigen Security Awareness Trainings für die gesamte Belegschaft.

Ab Q1/2022 – Awareness Trainings beim Rhein-Kreis Neuss

Mit „Security Awareness Trainings“ und Phishing Simulationen wird erlernt, wie getarnte Hackeraktivitäten am eigenen Rechner, bei E-Mails und im Internet zu erkennen sind.

Der Rhein-Kreis Neuss führt deshalb in 2022 ein für alle Mitarbeiterinnen und Mitarbeiter verpflichtendes, Web-basiertes Sicherheits-Trainingsprogramm ein. Die Anwender werden durch spezielle Lernmodule auf das Erkennen von IT-Sicherheitsgefahren vorbereitet.

„Microtrainings“ mit geringem Zeitaufwand

Das notwendige Wissen wird über sogenannte „Microtrainings“ vermittelt. Diese innovative Lernmethode gibt die Möglichkeit, flexibel und mit einem geringen Zeitaufwand zur selbst gewünschten Zeit zu lernen.

Dafür werden die Beschäftigten über eine spezialisierte Lernpattform zu kleinen Informationseinheiten eingeladen.

Der Lernerfolg soll langfristig, aber nachhaltig erreicht werden. Wenige Minuten in der Woche reichen aus, um ein gutes Grundwissen für die notwendige IT-Sicherheit zu erreichen.

Automatisierte Lernabläufe

Zu den Trainings und dem persönlichen Lernerfolg wird über E-Mails informiert. Anwender erhalten vom Lernprogramm verschiedene Nachrichten, Zwischenberichte zum Lernerfolg und Zusammenfassungen zu den Lerninhalten. Einladungen zu Tests erfolgen automatisch auf der Grundlage der eigenen Fortschritte.

Microtrainings beeinflussen die Lernkurve nachhaltig. Sie steigern die Trainingsmotivation, bringen Zeitersparnis und unterstützen die Umsetzung von Verhaltensänderungen.

Der Ansatz für erfolgreiche Awareness Trainings
Lernmodule als Microtraining Module

Schritt 1

Ein Gleichgewicht zwischen dem angezielten Sicherheitsniveau und der benötigten Zeit ist erforderlich.

Schritt 2

Der Schulungsablauf sollte automatisiert werden.

Mitarbeiter müssen nach eigenem Tempo lernen können.

Schritt 3

Echtzeitprognosen machen die Schulungsziele überprüfbar.

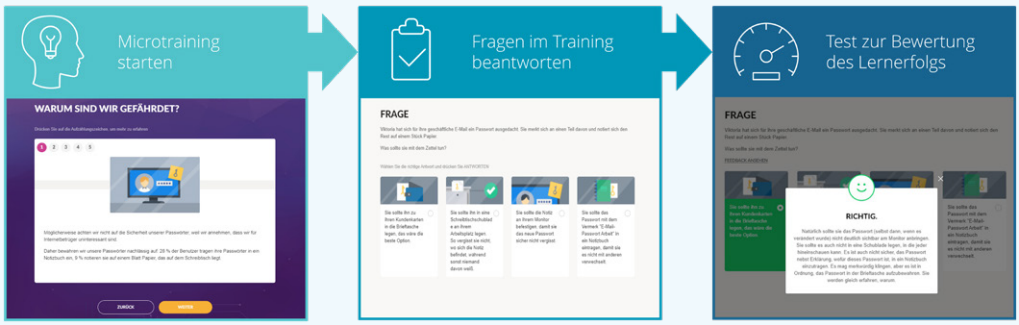
Eventuell brauchen bestimmte Fachbereiche mehr Aufmerksamkeit.

Schritt 4

Praktische, interaktive Übungen müssen zum Lernen motivieren.

Informationsüberflutung und Weiterbildungsmüdigkeit sind zu vermeiden.

Um die Schulungsziele zu erreichen sollen die Beschäftigten das Lerntempo selbst beeinflussen. Ein Lernporgramm mit hoher Akzeptanz erreicht einen nachhaltigen Lernerfolg.



Vom Start bis zum Wissenstest:
Die Beschäftigten beim Rhein-Kreis Neuss werden automatisch durch das Lernprogramm geführt.

Security Operation Center für die Cybersicherheit

Proaktive Überwachung von Systemereignissen

Der Schutz vor Cyber-Angriffen braucht Experten

Auch bei einer gut vorbereiteten Cybersicherheitsstrategie lassen sich durch Schwachstellen ständig Lücken in der IT-Abwehr finden, die irgendwann ausgenutzt werden. Den darauf basierenden Angriffen müssen menschliche Cyber-Security-Spezialisten gegenüberstehen.

Dauerhafte Sicherheit hängt von Experten ab, die proaktiv nach Gefahren suchen, Lücken frühzeitig schließen oder im Ernstfall rechtzeitig eingreifen. Eine ganzheitliche Überwachung, womöglich 24 Stunden am Tag, ist durch die IT-Security Fachkräfte vor Ort kaum selbst zu leisten. Experten-Teams eines “Security Operation Centers” (SOC) mit “Managed-Detection-and-Response-Diensten” (MDR) sind eine effiziente Ergänzung zu den internen Sicherheitsteams. Sie bieten den notwendigen Schutz gegen mögliche Attacken, auch außerhalb der Kernarbeitszeiten einer Kommune.

Ein SOC bewertet gesammelte Daten

Die Arbeit der Experten in einem SOC basiert auf Informationen von Systemereignissen und Datenquellen, die teils automatisiert interpretiert werden. Indexwerte zeigen, wie stark Systeme kompromittiert sind und wo Angriffe unmittelbar bevorstehen. Die notwendigen Informatonen werden in einem Security Information and Event Management (SIEM) zusammengeführt. Experten haben damit permanent die IT-Sicherheit eines Kunden im Blick.

Risikobewertung und Abwehr

Eine effektive Cyberabwehr kann nur im Team gelingen. Erste Ansprechpartner sind die Security Account Manager. Sie sind die Brücke zwischen Kunden und einem Expertenteam. Sie bewerten alle Informationen und veranlassen spezielle Recherchen, das Erstellen von Risikoprofilen oder die Definition von Abwehrmaßnahmen durch andere Sicherheitsanalysten.

Darüber hinaus greift der Security Manager auf verschiedene andere Teams technischer Spezialisten zurück: Eine Gruppe interpretiert aktuelle Sicherheitsalarme. Andere entwickeln individuell für den Kunden die Risikoprofile. Sie entwerfen zudem kundenspezifische Kataloge mit Sofortmaßnahmen für den Ernstfall.

Aufbau eine kontinulierichen SOC Betreuung

Der Rhein-Kreis Neuss strebt den kombinierten Einsatz eines zentralen Sicherheits-Monitorings mit der Unterstützung duch ein externes SOC Team für 2022 an. Der strukturelle Aufbau ist ein mittelfristiger Prozess, um die individuelle Sicherheitslage und den Normalbetrieb des Rhein-Kreises Neuss detailliert zu erfassen. Darauf aufbauend definieren die Spezialisten die IT-Abläufe und Maßnahmen für den Rhein-Kreis Neuss.

Mit der Einführung von „SOC as a Service“ und einem zentralen Monitoring wird die IT-Überwachung beim Rhein-Kreis Neuss nachhaltig gestärkt.

SOC-as-a-service

Die elementaren Bausteine für den Betrieb eines SOC Supports

Emergency Response Service	Umfassende Unterstützung bei der Schadens–eindämmung und Forensik bei einem Sicherheitsvorfall
Security Monitoring	Kontinuierliche Überwachung und Analyse von Sicherheitsvorfällen durch Security Spezialisten inkl. Alarmierung
Network Traffic & Behavior Analysis	Anreicherung der Security Intelligence Plattform mit Netzwerkfluss-Daten
Security Intelligence Plattform	Bereitstellung und Betrieb einer zentralen Security Event Management und Analyse Plattform

Die Funktionsweise

Security Intelligence Platform

Für die Erkennung und Analyse von Sicherheitsvorfällen wird in der IT Infrastruktur eine Security-Intelligence-Lösung implementiert. Sicherheitsrelevante IT-Ereignisse werden erfasst und auf die Übereinstimmung mit Bedrohungsinformationen überprüft. Dadurch lassen sich bekannte Gefahren erkennen als auch Anomalien identifizieren, die auf bisher unbekannte Angriffe hindeuten.

Security Monitoring

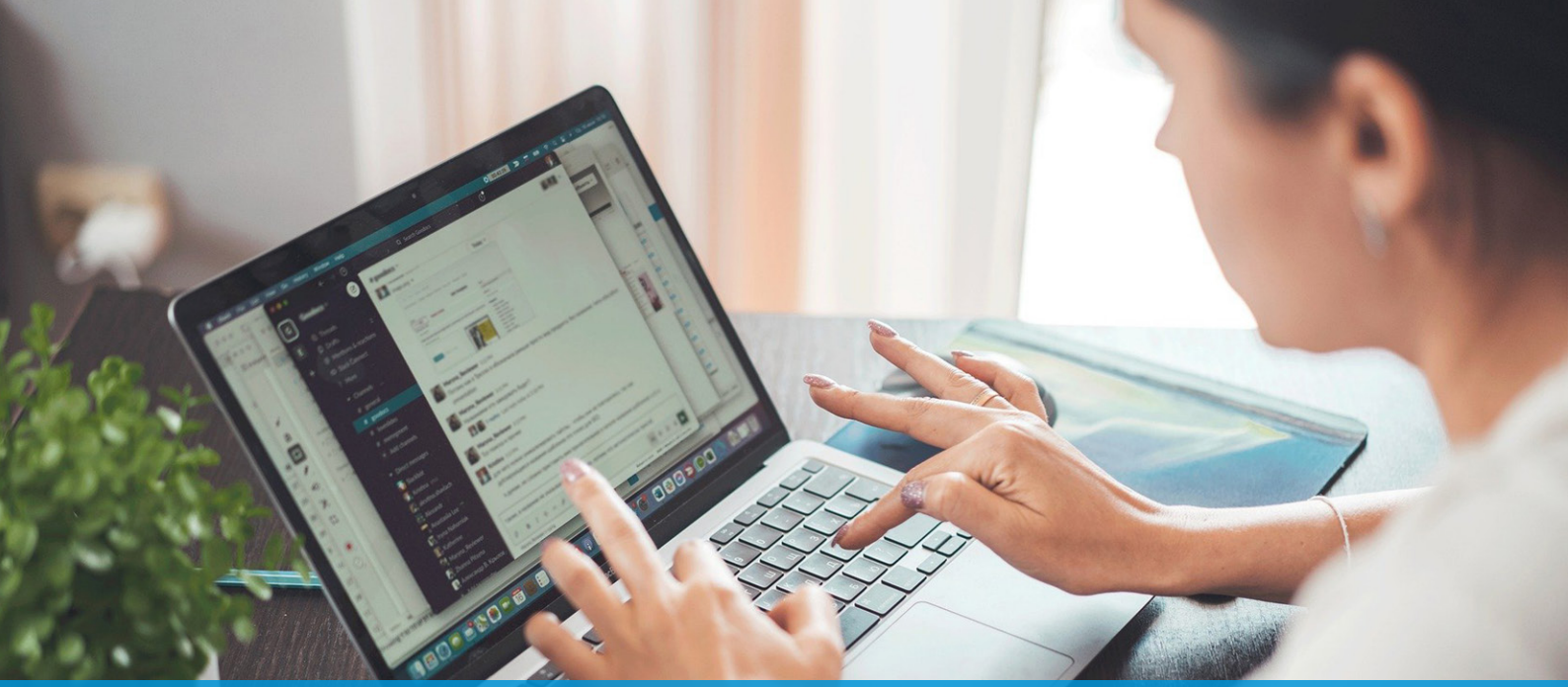
Security-Spezialisten überwachen alle Vorfälle, die durch die Security Intelligence Platform identifiziert werden. Eine Anreicherung mit Informationen aus Threat-Intelligence-Quellen sowie die manuelle Analyse des SOC Teams liefern eine Einschätzung, ob es sich um einen sicherheitsrelevanten Vorfall handelt.

Network Traffic & Behaviour Analysis

Durch den Einsatz von Flow-Prozessoren erfolgt eine ergänzende Überwachung und Analyse von Netzwerk-flussdaten. Durch die Korrelation dieser Netzwerkflussdaten mit den Ereignisdaten können mehr Gefährdun-gen erkannt werden als bei der ausschließlichen Konzentration auf Ereignisdaten.

Emergency Response Service

Im Falle eines Security Incidents müssen Maßnahmen zur Schadenseindämmung eingeleitet werden. Beim Er-fassen, Sichern und Analysieren von Spuren werden forensische Verfahren eingesetzt, um die Ursache und das Ausmaß des Vorfalls bestimmen sowie geeignete Gegenmaßnahmen einleiten zu können. Nach Abschluss des Einsatzes erfolgt ein detaillierter Bericht, mit Empfehlungen zur Abstellung der Angriffsfläche.



IT-Sicherheit auch aus dem Homeoffice

IT-Sicherheitsvorgaben für das Homeoffice

Ortsunabhängiges Arbeiten hat durch die Corona-Krise einen besonderen Aufschwung erfahren. Das mobile Arbeiten muss unter den Vorgaben der IT-Sicherheit ermöglicht werden. Was vor Zeiten der Pandemie noch für wenige Telearbeitsplätze galt braucht inzwischen einen generellen Sicherheitsstandard, um mobiles Arbeiten in der Breite aufrecht zu erhalten. Wenn Mitarbeiterinnen und Mitarbeiter des Rhein-Kreises Neuss jenseits der gut geschützten zentralen Infrastruktur arbeiten, wirft das zusätzliche Sicherheitsfragen auf.

Physikalische Sicherheit im Homeoffice

Das Büro beim Rhein-Kreis Neuss bietet auch bei Publikumsverkehr einen gut geschützen Arbeitsbereich. Zuhause liegt es in der eigenen Verwantwortung, den Zugriff auf den Rechner, das Einsehen von Daten durch Dritte und die Verarbeitung von gedruckten Dokumenten mit sensiblen Informationen sicher zu regeln. Mobiles Arbeiten erfordert eigene Vorgaben und Regeln, die teils von den Vorschriften im Büro abweichen.

Unsichere Netzwerke

Grundsätzlich werden beim Arbeiten aus dem Homeoffice Netzwerke genutzt, die nicht der Kontrolle der IT-Verwaltung unterliegen. Diese als unsicher betrachteten Netzwerke müssen über zertifizierte und gesicherte Verbindungen zum Verwaltungsnetz kontaktieren. Gleichzeitig muss gewährleistet sein, dass die Internetverbindung des Anwenders stabil ist und genügend Bandbreite bietet, damit er seine Leistung angemessen erbringen kann. Auch das ist eine Frage der Informationssicherheit. Denn sonst wird eines der drei Schutzziele, nämlich die Verfügbarkeit von Daten sicherzustellen, nicht erreicht. Die beiden anderen Schutzziele sind die Vertraulichkeit und die Integrität von Informationen sicherzustellen.

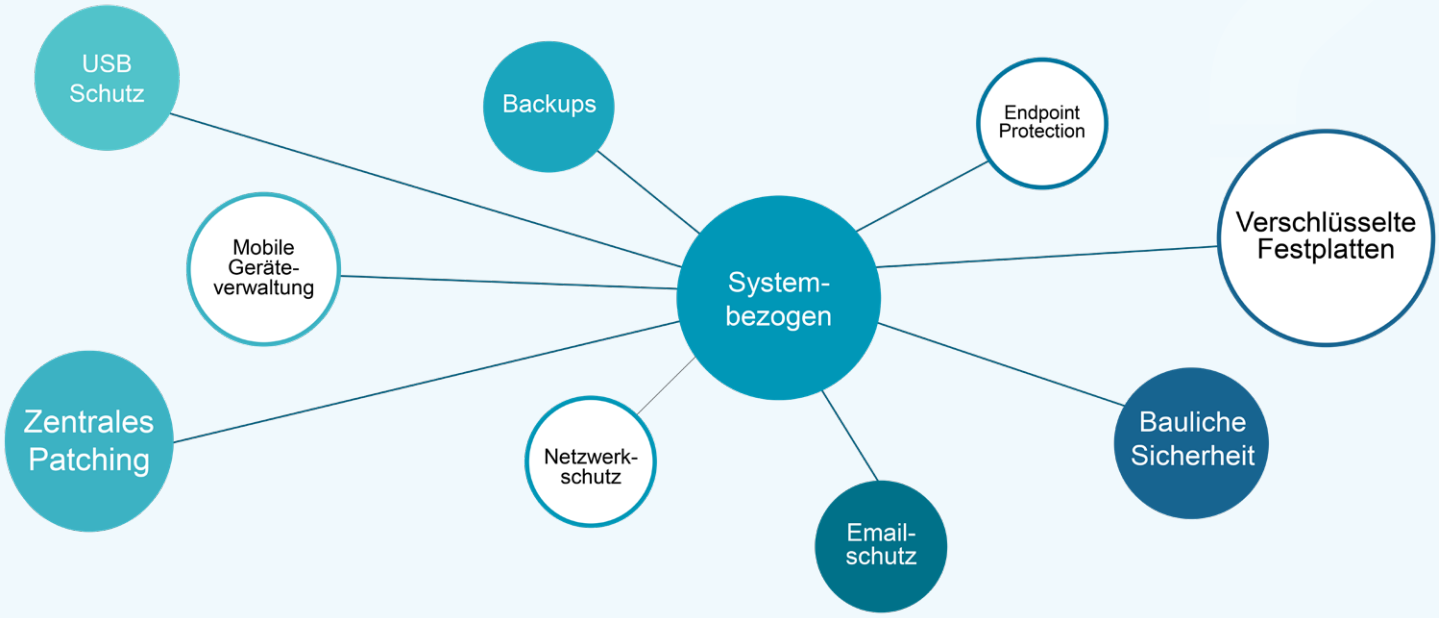
Risiken durch Cyber-Angriffe

Angriffsszenarien im Homeoffice unterscheiden sich nicht wesentlich von denen in Unternehmensumgebungen. Besonders häufig kommen Malware- und Phishing-Attacken vor. Im Homeoffice sind Beschäftigte anfälliger für solche Attacken, denn zuhause fällt bei eigener, isolierter Entscheidung die Einschätzung von Risiken eventuell anders aus.

Client-seitige Schutzmaßnahmen

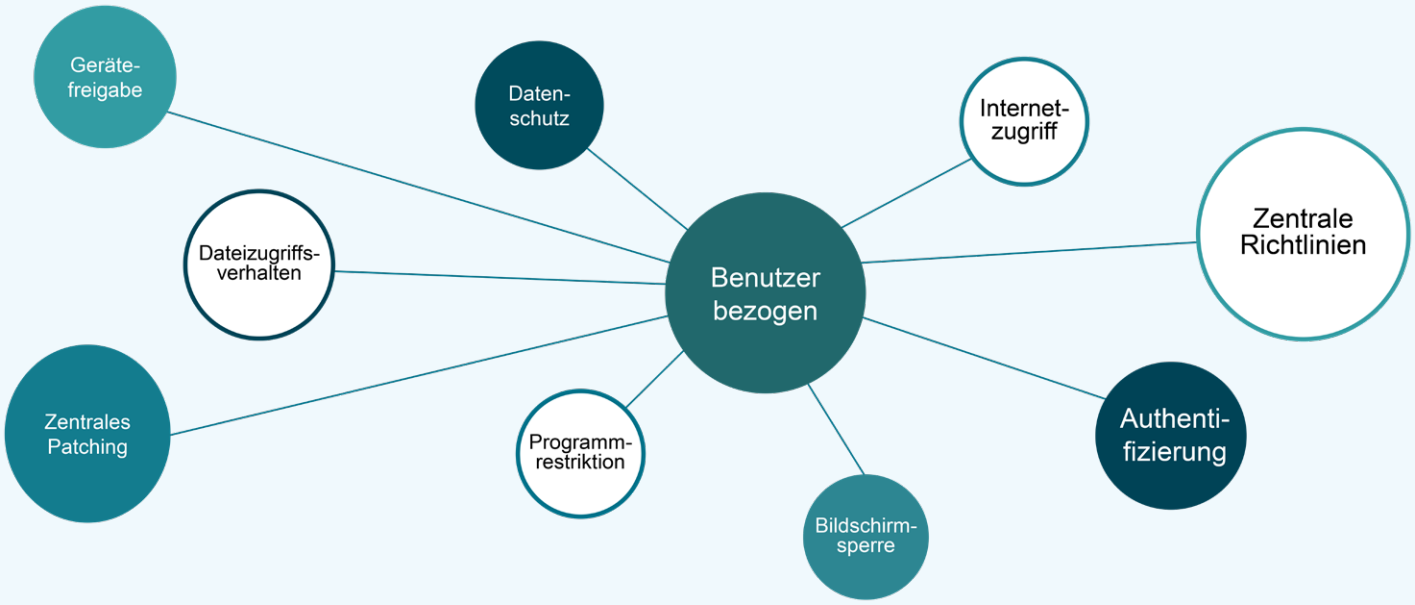
Endgeräte im Homeoffice müssen konsequent mit den gängigen Cyber-Security-Techniken geschützt werden. Dazu gehören zum Beispiel eine Endpoint Protection-Lösung, eine Firewall und Media-Encryption. Festplattenverschlüsselung schützt vor unbefugten Zugriffen, wenn ein Laptop verloren geht. Notwendig sind auch ein URL-Filter und eine Applikationseinschränkung. Verdächtige Ereignisse müssen automatisch an den zentralen IT Support gemeldet werden.

Schutzmaßnahmen bei Hard-und Software



Die IT-Verwaltung des Rhein-Kreises Neuss nimmt zahlreiche Einstellungen und Restriktionen vor, um Systeme wie Netzwerke, Server, Datenspeicher, PCs und Notebooks vor Angriffen zu schützen.

Benutzer- und Zugriffsrechte



Benutzer unterliegen beim Rhein-Kreis Neuss einer Vielzahl von Regeln, um sicher arbeiten zu können.

Cyber-Risiken 2022

Wie entwickelt sich die Bedrohungslage?

Prognose zu Cyber-Risiken

Um sich bestmöglich auf die Gefahren durch Cyber-Kriminelle einzustellen muss bewusst sein, inwieweit sich ein verändertes Angriffsverhalten oder neue kriminelle Technologien erkennen lassen. Gerade im Bereich von Cyber-Risiken fällt es aber schwer abzuschätzen, welche Bedrohungen in den nächsten Wochen und Monaten vorherrschen werden.

Berichte wie zum Beispiel vom Versicherer Allianz Global Corporate & Speciality (AGCS) liefern gute Anhaltspunkte, wie sich Cyber-Risiken entwickeln könnten. ACGS berichtet, dass Cyber-Vorfälle eine der Hauptgefahren für Unternehmen darstellt. Die durch die Pandemie getriebene Beschleunigung hin zu mehr Digitalisierung und Homeoffice verschärfe die IT-Schwachstellen auffallend weiter.

Angreifer nutzen Covid-19

Durch Covid-19 haben sich neue Möglichkeiten für Angriffe entwickelt. Zunehmend wird durch Hacker automatisiertes Scannen genutzt, um Sicherheitslücken zu erkennen. Schlecht gesicherte Router sind für viele Angreifer das notwendige Einfallstor in Netzwerke. Durch künstliche Intelligenz lassen sich Medieninhalte gezielt manipulieren. Die Auswirkungen reichen von bewusster Desinformation und Propaganda bis zur gezielten Diskreditierung einzelner Personen.

Lehren aus der Pandemie ziehen

In der Pandemie sind allein in Deutschland zwölf Millionen Berufstätige ins Homeoffice gewechselt. Laut einer BSI Umfage aus dem Jahr 2021 nutzten aber nur 42 Prozent der Unternehmen ausschließlich eigene IT.

Mobiles Arbeiten wird dauerhaft die neue Normalität bestimmen. Es bedarf einer richtigen Balance zwischen dem benutzerfreundlichen Zugriff auf die Behördendaten und dem Schutz der IT. Der Corona-bedingte Digitalisierungsschub hat die mögliche Angriffsfläche und damit das Risiko erfolgreicher Cyberangriffe erheblich vergrößert.

Internetkriminelle passen sich schnell an

Cyberkriminelle haben flexibel auf die Pandemie reagiert und die allgemeine Verunsicherung gezielt ausgenutzt. Die gesteigerte Aggressivität der Erpressungsmethoden bei Ransomware-Angriffen sowie professionelle Angriffe auf zahlungskräftige Ziele haben sich weiter verstärkt.

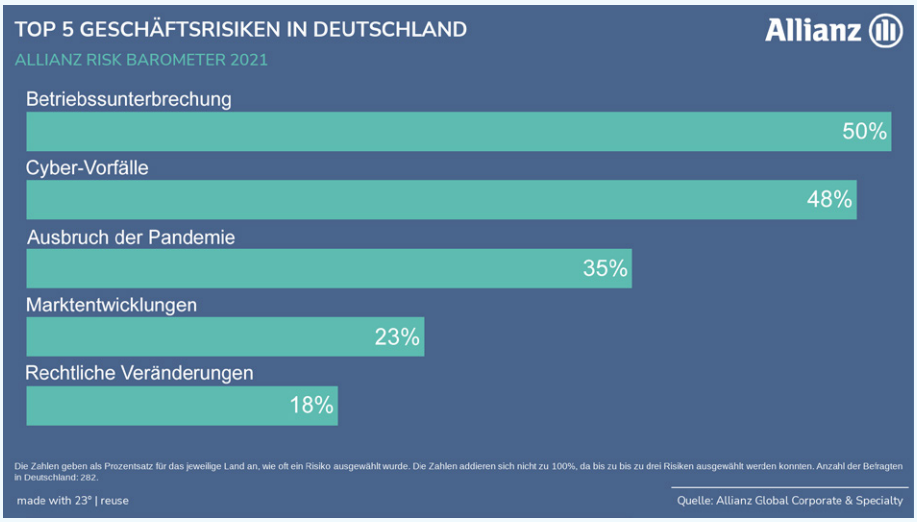
In IT-Sicherheit investieren

Über 50 Prozent der Unternehmen investieren weniger als zehn Prozent der IT-Ausgaben in Cybersicherheit. Das BSI empfiehlt, bis zu 20 Prozent des IT-Budgets in Sicherheit zu investieren. Die zusätzlichen Sicherungsmaßnahmen brauchen zudem eine personelle Stütze.

Laut einer Umfrage der Allianz Global Corporate & Speciality waren

- Betriebsunterbrechung
- Pandemie -Ausbruch
- Cyber-Vorfälle

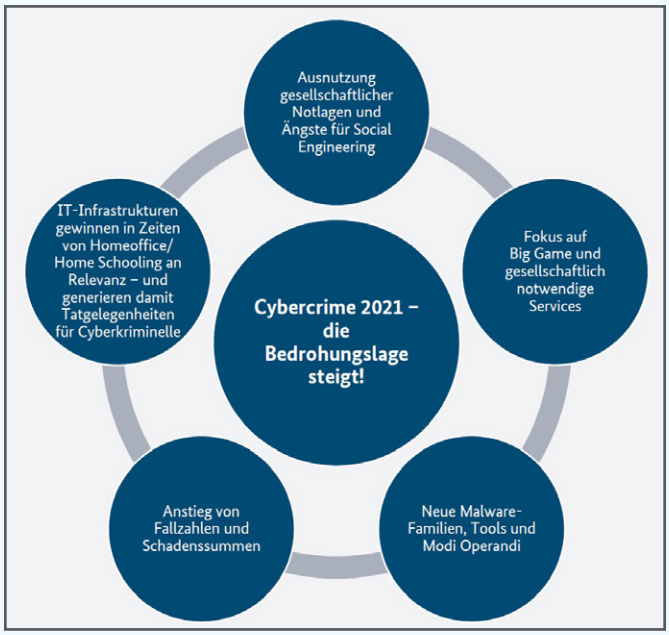
die drei wichtigsten Geschäftsrisiken für 2021.



Im "Bundeslagebild Cybercrime" gibt das BKA einen Ausblick zu den weiteren Entwicklungen im Cybercrime:

- IT-Infrastrukturen gewinnen in Zeiten von Homeoffice an Relevanz und generieren damit Tatgelegenheiten für Cyber-Kriminelle.

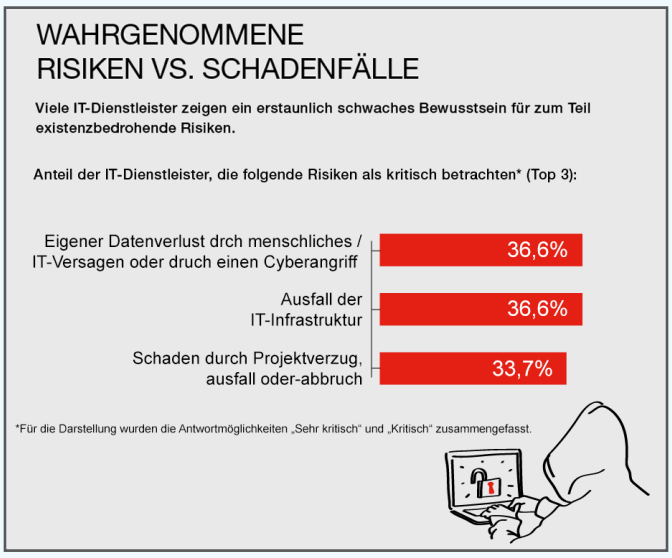
- Gesellschaftliche Notlagen und Ängste werden vermehrt für Social Engineering ausgenutzt.



Risikowahrnehmung und Realität:

Im Auftrag des Spezialversicherers Hiscox äußerten sich IT-Dienstleistungsunternehmen zu ihrer aktuellen Lage und der Wahrnehmung unternehmerischer Risiken.

Angesichts der vielfältigen Risiken setzen IT-Dienstleister verhältnismäßig wenig auf Absicherung durch eine Versicherung.



IT Riskikomanagement
mit CVE Schwachstellen Scans

Was sind Common Vulnerabilities and Exposures (CVE)?

Bei Common Vulnerabilities and Exposures (CVE) handelt es sich um bekannte Schwachstellen und Sicherheitsrisken in IT-Systemen. Die Sicherheitslücken werden gemeldet, erfasst und in einer standardisierten Form mit laufender Nummer benannt. Jeder Schwachstelle wird ein Score verliehen, der den Schweregrad zur Sicherheitslücke angibt.

Wie werden Software-Schwachstellen von Cyber-Kriminellen ausgenutzt?

Das Ausnutzen von Sicherheitslücken in IT-Systemen wird Exploit genannt. Dabei nutzen Hacker gezielt diese Schwachstellen aus. Ein Großteil der Angriffe findet auf bekannte Schwachstellen (CVE) statt, für die eigentlich schon Patches zu Verfügung stehen. Angreifer scannen Systeme gezielt nach offenen Schwachstellen, wodurch die Angreifer in der Lage sind, schadhaft auszunutzen.

Was bedeutet Schwachstellenmanagement?

Schwachstellenmanagement ist ein Prozess der IT-Sicherheit, der darauf abzielt, Sicherheitslücken in der IT-Infrastruktur zu finden, ihren Schweregrad einzustufen und Maßnahmen auflistet, um diese Schwachstellen zu beheben. Ziel ist es, die Probleme zu eliminieren, sodass der daraus mögliche Schaden abgewendet wird .

Welche Vorteile bringt ein Schwachstellen Scan?

Die laufende Statistik belegt: 999 von 1.000 Schwachstellen sind bereits über ein Jahr bekannt. Diese Schwachstellen können erkannt und beseitigt werden, bevor sie von Angreifenden ausgenutzt werden. Das Auffinden und Abstellen der Sicherheitslücken reduziert die Angriffsfläche auf die IT-Infrastruktur erheblich.

CVE in der eigenen IT-Infrastruktur finden

Die beim Rhein-Kreis Neuss eingesetzte Patch Verwaltung soll durch ein qualifiziertes Schwachstellenmanagement ergänzt werden. Dies ist kein einmaliger Vorgang, sondern ein andauernder Prozess, der fest in die IT-Sicherheit integriert wird. Die Schritte von der Erkennung bis zur Behebung von Schwachstellen laufen kontinuierlich in einem beständigen Kreislauf ab.

Die wiederkehrenden Suchläufe nach Schwachstellen unterstützen die IT des Rhein-Kreises Neuss bei der priorisierten Bearbeitung und der Erkennung von Sicherheitslücken, auf die bereits reagiert werden kann. Der Status Quo der Riskoanfälligkeit wird hiermit kontinuierlich reduziert.

Ein solcher Scanprozess wird offensichtliche Nacharbeiten zur Absicherung der IT-Produkte erforderlich machen. Das bindet zusätzliche personelle Ressourcen, trägt dafür im Gegenzug zu einer besonderes hohen Systemstabilität bei.

Der Kreislauf beim Schwachstellenmanagment

Das Schwachstellenmanagement folgt einem immer wiederkehrenden Kreislauf:

- Nach der Erkennung einer Schwachstelle muss deren Bearbeitung mit einer Priorität versehen und die Auswirkung bewertet werden.
- Der Zustand wird in einem Bericht festgehalten.
- Die Schwachstelle wird behoben.
- Das Aktualisieren wird überprüft.
- Die gesammelten Informationen bilden die Basis für die nächste Runde im ununterbrochenen Aktualisierungskreislauf.

Glossar

APT
Advanced Persistent Threat (APT) zu deutsch „fortgeschrittene, andauernde Bedrohung“ ist ein häufig im Bereich der Cyber-Bedrohung (Cyber-Attacke) verwendeter Begriff für einen komplexen, zielgerichteten und effektiven Angriff auf kritische IT-Infrastrukturen und vertrauliche Daten von Behörden, Groß- und Mittelstandsunternehmen aller Branchen, welche aufgrund ihres Technologievorsprungs potenzielle Opfer darstellen oder als Sprungbrett auf solche Opfer dienen können.

Awareness
Engl. „Bewusstsein“ oder „Gewahrsein“, auch übersetzt als „Bewusstheit“, zur Betonung der aktiven Haltung bzgl. IT-Sicherheit, auch „Aufmerksamkeit“.

Big Game Hunting
Der Prozess von Cyberkriminellen, die sich auf hochwertige Daten oder Assets innerhalb von Unternehmen konzentrieren. Die Ziele werden so ausgewählt, von denen davon ausgegangen wird, dass diese empfindlich auf Ausfallzeiten oder Data-Breaches reagieren Lösegeld bezahlen.

Botnetz
Ein Botnet oder Botnetz ist eine Gruppe automatisierter Schadprogramme, sogenannter Bots. Die Bots (von englisch: robot „Roboter“) laufen auf vernetzten Rechnern, deren Netzwerkanbindung sowie lokale Ressourcen und Daten ihnen, ohne Einverständnis des Eigentümers, zur Verfügung stehen.

CVE
Bei Common Vulnerabilities and Exposures (CVE) handelt es sich um bekannte Schwachstellen und Sicherheitsrisken in IT-Systemen. Die Sicherheitslücken werden gemeldet, erfasst und in einer standardisierten Form mit laufender Nummer benannt.

Cyber-Angriff
Ein Cyber-Angriff ist eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyber-Raum, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen.

Darknet
englisch für „Dunkles Netz“; beschreibt in der Informatik ein Peer-to-Peer-Overlay-Netzwerk, dessen Teilnehmer ihre Verbindungen untereinander manuell herstellen.

Datenschutz
Mit Datenschutz wird der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet (nicht zu verwechseln mit Datensicherheit).

DDoS
Denial of Service (DoS; engl. für „Verweigerung des Dienstes“) bezeichnet in der Informationstechnik die Nichtverfügbarkeit eines Internetdienstes, der eigentlich verfügbar sein sollte. Häufigster Grund ist die Überlastung des Datennetzes. Das kann unbeabsichtigt verursacht werden oder durch einen konzentrierten Angriff auf die Server oder sonstige Komponenten des Datennetzes erfolgen.

E-Mail Gateway
Ein E-Mail Gateway kontrolliert E-Mails, die an eine Organisation gesendet werden, auf unerwünschte Inhalte und verhindert, dass diese Nachrichten zugestellt werden.

Firewall
Eine Firewall ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt. Eine Firewall gewährleistet die sichere Kopplung von IP-Netzen und sorgt dafür, dass ausschließlich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen werden.

Gruppenrichtlinien
Die Gruppenrichtlinien haben ihren Namen nach die Aufgabe, zentrale IT-Vorgaben verbindlich im Unternehmen umzusetzen. Ihre typischen Anwendungen bestehen darin, Desktops gegen Änderungen durch die User zu schützen, Sicherheitseinstellungen zentral festzulegen, Software zu verteilen oder Anwendungen zu konfigurieren.

Informationssicherheits-Management-System (ISMS)
Das ISMS ist eine Aufstellung von Verfahren und Regeln innerhalb eines Unternehmens, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Internet-of-Things
Das Internet der Dinge (IdD) ist ein Sammelbegriff für Technologien einer globalen Infrastruktur der Informationsgesellschaften, die es ermöglicht, physische und virtuelle Gegenstände miteinander zu vernetzen und sie durch Informations- und Kommunikationstechniken zusammenarbeiten zu lassen.

KRITIS
Kritische Infrastrukturen sind Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall nachhaltig Versorgungsengpässe oder erhebliche Störungen eintreten würden.

Kryptowährung
Eine Kryptowährung ist ein digitales Zahlungsmittel, das mit Prinzipien der Kryptographie erstellt und transferiert wird.

Malware
Als Schadprogramm, Schadsoftware oder Malware (Kofferwort aus malicious ‚bösartig' und software) bezeichnet man Computerprogramme, die entwickelt wurden, um unerwünschte und gegebenenfalls schädliche Funktionen auszuführen. Malware ist damit ein Oberbegriff, der u. a. das Computervirus umfasst.

Mircrotraining
Als kurze Trainingseinheit beschreibt es ein Lernformat, das dem Austausch von Infos, der Wissensvermittlung und der Weiterbildung der Mitarbeiter dient.

Outlook-Harvesting
Erzeugen authentisch wirkender Spam-Mails anhand ausgelesener E-Mail-Inhalte und Kontaktdaten bereits betroffener Nutzer.

Phishing
Das Wort setzt sich aus „Password" und „Fishing" zusammen, zu Deutsch „nach Passwörtern angeln". Beim Phishing wird z. B. mittels gefälschter E-Mails und/oder Webseiten versucht, Zugangsdaten für einen Dienst oder eine Webseite zu erlangen.

Proxy
Ein Proxy ist eine Art Stellvertreter in Netzen. Er nimmt Daten von einer Seite an und leitet sie an eine andere Stelle im Netz weiter. Mittels eines Proxys lassen sich Datenströme filtern und gezielt weiterleiten.

Ransomware
Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch „ransom") wieder freigeben.

Reputation
Die Reputation des Absenders einer E-Mail ist entscheidend für den Filter und damit für die Frage, ob eine E-Mail durchkommt oder blockiert wird. In die Bewertung der Reputation eines Absenders fließen verschiedene Kennzahlen ein (Reputationsmanagement).

Schadprogramm / Schadsoftware / Malware
Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Beispiele sind Computer-Viren, Würmer und Trojanische Pferde.

Schadprogramm / Schadsoftware / Malware
Ein Snapshot ist ein besonderer Speicherbereich, der ältere oder jüngere Versionen geänderter Daten aufnimmt. Er enthält keine vollständige Kopie des Datenbestands, sondern wird bei jeder Änderung schrittweise gefüllt.

SOC
Beim Security Operations Center (SOC) handelt es sich um eine Sicherheitsleitstelle, die sich um den Schutz der IT-Infrastruktur eines Unternehmens oder einer Organisation kümmert. Um diese Aufgabe leisten zu können, integriert, überwacht und analysiert das SOC alle sicherheitsrelevanten Systeme.

Spam
Unter Spam versteht man unerwünschte Nachrichten, die massenhaft und ungezielt u.a. per E-Mail versendet werden. In der harmlosen Variante enthalten SpamNachrichten meist unerwünschte Werbung, häufig jedoch auch Schadprogramme im Anhang, Links zu verseuchten Webseiten etc.

Spyware
Bei Spyware handelt es sich um eine Software, die ohne Wissen des Anwenders Aktivitäten auf dem Rechner oder im Internet ausspioniert und aufzeichnet.

Trojaner
Ein Trojaner ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Ein Trojaner verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.

Viren
Klassische Form von Schadsoftware, die sich selbst verbreitet und unterschiedliches Schadpotenzial in sich tragen kann. Viren treten in Kombination mit einem Wirt auf, z. B. einem infizierten Dokument oder Programm.

VPN
Ein Virtual Private Network (VPN) ermöglicht eine verschlüsselte, zielgerichtete Übertragung von Daten über öffentliche Netze wie das Internet. Es etabliert geschützte und in sich geschlossene Netzwerke mit verschiedenen Endgeräten. Häufige Anwendung ist die Anbindung von Home Offices oder mobilen Mitarbeitern.

Jahresbericht
IT-Sicherheit 2021/2022

Bildinhalte / Quellen

Allianz Global Corporate & Speciality (S.19)
Bundesamt für Sicherheit
in der Informationstechnik (BSI) (S.4,5,7)
Bitdefender (S.4)
Bundeskriminalamt (S.19)
Hiscox (S.19)
Kaspersky (S.13)
Pixabay.com - CCO Lizenz (S.6,8,10,11,12,14,16,18,20)
Proofpoint (S. 12,15)
Security Insider (S.16,18)
Sophos GmbH (S.11)
Rhein-Kreis Neuss (S.7,9,12,21)

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