rhein kreis neuss

Jahresbericht

IT-Sicherheit

Rückblick 2019

Ausblick 2020

Vorwort

Laut Zahlen des Bundesamts für Sicherheit in der Informationstechnik (BSI) wurden in den vergangenen zwei Jahren ca. 70 Prozent aller Unternehmen und Institutionen in Deutschland Opfer von Cyber-Angriffen. In knapp der Hälfte der Fälle waren die Angreifer erfolgreich. Allein diese Zahl macht deutlich, dass man heutzutage intensiver als in den Vorjahren kombinierte Maßnahmen für eine höchstmögliche IT Sicherheit vorbereiten muss.

Maßgaben wie die Verwendung sicherer Kennwörter, das Sperren des PCs oder Abschließen des Büros bei Abwesenheit, um den unbefugten Zugriff auf Daten zu verhindern, sowie ein Online-IT-Sicherheitstraining für alle Mitarbeiter/innen sind nur ein Teil der Schutz- und der Sensibilisierungsmaßnahmen in unserer Kreisverwaltung. Unverzichtbar bleibt beim Thema Sicherheit auch die enge Zusammenarbeit mit der ITK Rheinland.

Die potentiellen Angriffsmöglichkeiten sowie Risiken von Störungen nehmen mit der stetig fortschreitenden Vernetzung in einer digitalisierten Welt erheblich zu. Aktuelle Vorfälle zeigen immer wieder, dass es keinen vollständigen automatisierten Schutz vor Cyberangriffen gibt. Deshalb nimmt die Sensibilisierung und Fortbildung der Mitarbeiterinnen und Mitarbeiter eine wichtige Rolle ein.

Darüber hinaus steht Ihnen in der Kreisverwaltung bei allen Fragen rund um das Thema IT-Sicherheit Frank Meger als Ansprechpartner und IT-Sicherheitsbeauftragter der Kreisverwaltung zur Verfügung.

Der vorliegende Bericht gibt eine Übersicht über den aktuellen Status relevanter Themen und Maßnahmen im Jahr 2019 sowie einen Ausblick auf unsere Ziele für das Jahr 2020 ff. Zu den farblich blau markierten Fachbegriffen finden Sie Erläuterungen im Glossar.

Harald Vieten
Dezernent für IT, E-Government u. Bauen

Liebe Leserinnen und Leser,

Beachten Sie die seitlichen Zeitschienen, welche Status die verschiedenen Sicherheitsthemen beim Rhein-Kreis Neuss erreicht haben:

Fortsetzung 2020 **Update 2020**

Neu 2020/21

Lesen Sie diesen Bericht bitte in dem Bewusstsein, die IT-Sicherheit im Alltag zu leben und aktiv mitzugestalten. Der Weg zu einem weitreichenden Schutz führt ein entscheidendes Stück über uns alle.

Frank Meger
IT-Sicherheitsbeauftragter

Rhein-Kreis Neuss
Zentrale Steuerung ZS4
Lindenstraße 4
41515 Grevenbroich

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

Inhalt

Die Lage der IT-Sicherheit in Deutschland

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet die Gefährdungslage der IT-Sicherheit in Deutschland kontinuierlich und stellt hieraus einen jährlichen Bericht zusammen. Die Ergebnisse des Berichts für das Jahr 2019 werden im vorliegenden Artikel zusammengefasst.

Gefährdungslage

Der Schwerpunkt der IT Angriffe liegt aktuell im Bereich Cyber Kriminalität.

Beispiel 19. März 2019:
Das Unternehmen Norsk Hydro wird Opfer einer Ransomware Attacke. Festplatten werden verschlüsselt.

Über 50 Prozent aller Angriffe lösen solche Malware Infektionen aus.

Auch andere Gefährdungen haben immer noch einen hohen Gefährdungsanteil:

Identitätsdiebstähle, bei denen personenbezogene Daten missbräuchlich durch Dritte genutzt werden.
Botnetze sind auch wegen der zunehmenden Zahl mobiler Endgeräte und Internet-of-Things-Systemen aktiv.
Denial of Service (DDoS)-Angriffe nutzen spezialisierte neue Angrifsvektoren.
Spam Mails lassen nach, aber: Die Qualität und somit die Effektivität von Schadprogramm-Spam steigt weiterhin.

Erneut aktiv: Emotet

Eine im Berichtszeitraum besonders relevante Malware ist Emotet. Das schon seit 2010 bekannte Schadprogramm ist seit November 2018 wieder in neuen Varianten mithilfe von schädlichen Office-Dokumenten verteilt worden.

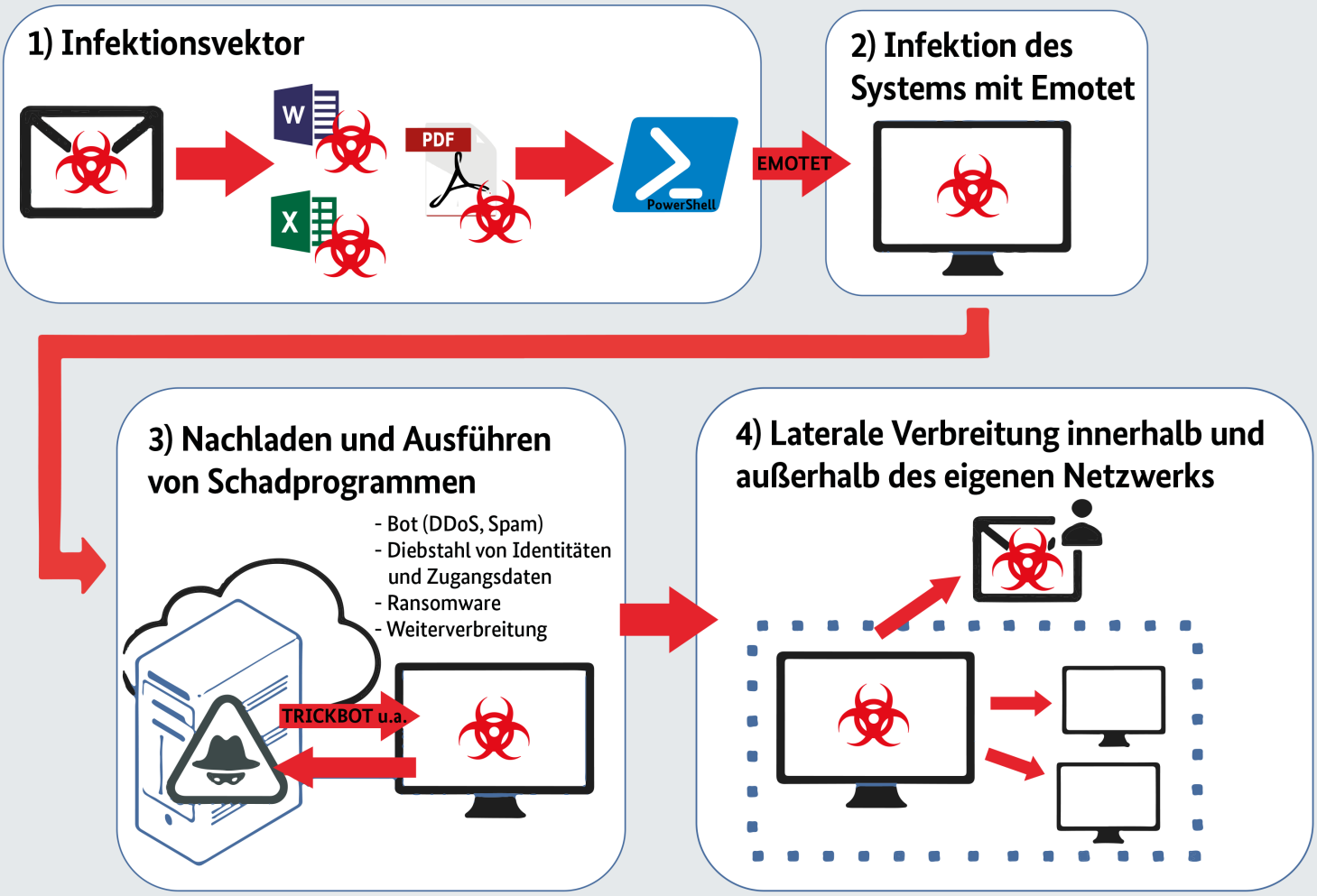
Neu war ab Herbst 2018, dass durch das „Outlook-Harvesting-Modul“ nicht nur die Kontaktbeziehungen, sondern auch E-Mail-Inhalte ausgespäht hat. Diese wurden aber erst im April 2019 verwendet, um noch authentischer aussehenden Spam zu versenden. Sobald ein Rechner durch Emotet infiziert ist, verwendet die Schadsoftware Kontaktbeziehungen und E-Mail-Inhalte aus den Outlook-Postfächern des infizierten Systems. Diese Informationen nutzen die Täter zur Verbreitung des Schadprogramms, sodass die Empfänger authentisch aussehende E-Mails von Absendern erhalten, mit denen sie kürzlich in Kontakt standen.

BSI & Verwaltung

Eine der Kernzielgruppen des BSI sind staatliche Stellen, insbesondere die Behörden des Bundes. Der Bedarf bei Behörden nach hochsicherer Verschlüsselung für die Erzeugung, Übermittlung und Speicherung vertraulicher Informationen wächst.

Im Zeitalter der Digitalisierung erwartet der Nutzer, sich hochsicher, unkompliziert und schnell austauschen zu können. Aus den sich entwickelnden Technologieansätzen entstehen Möglichkeiten zur Nutzung von für den staatlichen Geheimschutz konzipierten IT-Produkten in ganz neuen Einsatzfeldern. Das BSI unterstützt bei der Planung und Umsetzung.

Kommunalverwaltungen haben in vielen Fällen die gleichen Herausforderungen. Der Artikel „IT-Grundschutzprofil – Basis-Absicherung von Kommunalverwaltungen“ (ab Seite 8) gibt hierzu weitergehende Informationen.



Grafiken: https://www.fortinet.com/resources/icon-libary.html, Microsoft, Adobe

Mehrfacher Schadprogrammangriff

Auszug aus dem BSI Bericht 2019: „Dem BSI sind mehrere Fälle bekannt, in denen Ransomware nachgeladen und Unternehmensdaten verschlüsselt wurden. Die Folge waren Produktionsausfälle, ganze Unternehmensnetzwerke mussten neu aufgebaut werden."

Reaktion

Auch „kleinere" Infektionen durch eine in der Fläche verteilte Malware wie Emotet müssen unmittelbar behandelt und Zugangsdaten geändert werden, weil anderenfalls über diesen Eintrittsweg noch weitaus größere Schäden entstehen können.

Empfehlung

Sicherheitsupdates für Betriebssystem und Anwendungen müssen zietnah installiert werden. Regelmäßige Offline-Backups als auch das Monitoring und die Auswertung von Logdaten sind wichtig. Die nachhaltige Sensibilisierung von Nutzern gegen Social-Engineering sowie eine Netzsegmentierung von Produktions- und Büronetzwerken müssen berücksichtigt werden.

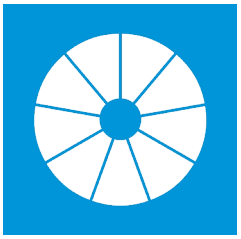
Weitere Informationen zu Emotet gibt es auf der Webseite „BSI für Bürger": https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/emotet.html

IT-Sicherheitsgesetz 2.0

Das IT-Sicherheitsgesetz 1.0 wird weiterentwickelt. Dabei soll das Bundesamt für Sicherheit in der Informationstechnik (BSI) deutlich mehr Befugnisse erhalten, um Sicherheitslücken aufzudecken und so die IT-Systeme von Gesellschaft, Wirtschaft und Behörden zu schützen.

Ende März 2019 wurde der Referentenentwurf zum IT-Sicherheitsgesetz 2.0 des Bundesministeriums des Innern fertiggestellt. Einen Überblick zum Referentenentwurf und den wesentlichen Änderungen finden Sie hier.

IT-SIG - Erweiterung KRITIS



Beim Thema Kritische Infrastrukturen (KRITIS) kommt der Bereich Abfallentsorgung zur Liste der Sektoren hinzu. Präzisiert wird die Kategorie „Infrastrukturen mit besonderem öffentlichen Interesse“. Sie beinhaltet nun die Bereiche Rüstungsindustrie, Prime Standard nach §48 Börsenordnung der Frankfurter Wertpapierbörse sowie Kultur und Medien.

IT-SIG - Cybersicherheit / IoT

Das BSI soll mit Rechten ausgestattet werden, die ein offensives Vorgehen gegen Botnetze, Risiken im Internet der Dinge und die Verbreitung von Schadsoftware ermöglichen. Das BSI soll die Befugnis erhalten, in fremde IT-Systeme einzudringen, um Patches zu installieren oder Schadsoftware zu entfernen. Es kann dann Providern anordnen, Datenverkehre zu blockieren oder umzuleiten, um Cyber-Angriffe abzuwehren.

IT-SIG - Gesetzesänderungen

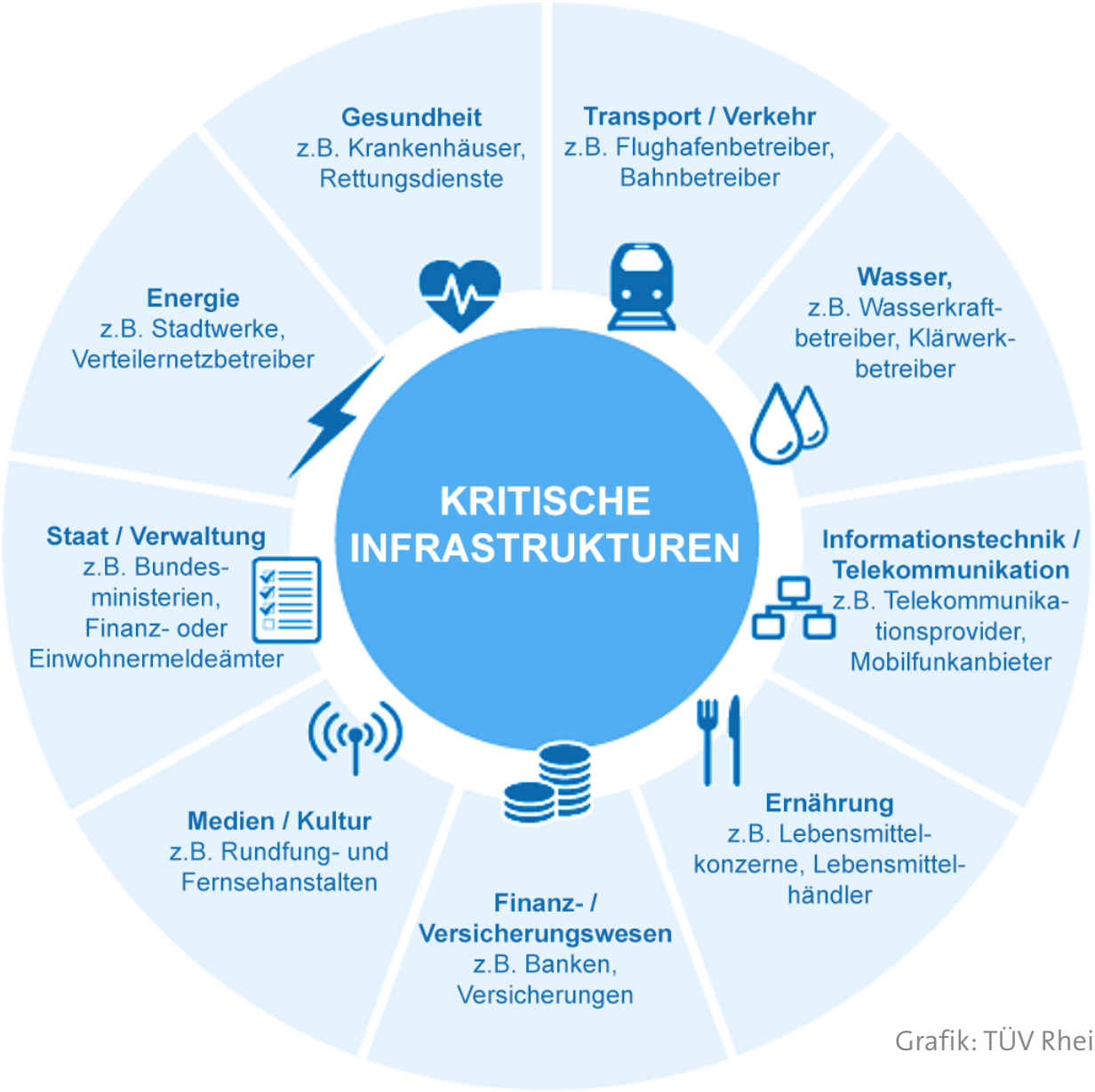
Der Entwurf beinhaltet zudem wesentliche Reformen des Telekommunikations- und Telemediengesetzes sowie des Strafgesetzbuches und der Strafprozessordnung. So werden Computerstraftaten zu „schweren Straftaten“ (§ 100a StPO) erklärt. Telekommunikationsdienste, die zur „Weitergabe oder Veröffentlichung rechtswidrig erlangter Daten“ genutzt werden, sollen verpflichtet werden, diese Daten zu sperren und zu löschen. Dies betrifft Anbieter wie z. B. Facebook, Google oder den Messenger Telegram.

Zusammengefasst

Der nun vorliegende Referentenentwurf zum IT-SiG 2.0 verfolgt einen ganzheitlichen Ansatz und enthält Maßnahmen zum Schutz der Bürger, zur Stärkung des Staates, zum Schutz der öffentlichen Informationstechnik und für eine informationstechnisch robuste Wirtschaft.

Das Gesetz stärkt vor allem die Rolle des BSI als zentrale Behörde mit weitreichenden Befugnissen. Dazu greift das Gesetz auch in das Straf- und das Strafverfahrensrecht ein. Neu ist die Übertragung von Aufgaben des Verbraucherschutzes an das BSI, das zukünftig mit „IT-Sicherheitskennzeichen“ die IT-Sicherheit von Produkten sichtbar machen sollen.

Neu ist auch, dass das BSI zukünftig Provider zum Löschen, zum Melden und zu Bestandsauskünften bei Cybercrime-Vorfällen verpflicheten kann.



Grafik: TÜV Rheinland

KRITIS - Kritische Infrastrukturen

Hersteller von Komponenten und Technik, die im KRITIS-Bereich eingesetzt werden, müssen künftig die Vertrauenswürdigkeit ihrer gesamten Lieferkette gewährleisten und hierzu eine Erklärung ihrer Vertrauenswürdigkeit gegenüber dem Betreiber abgeben.

Bestimmung von „KRITIS-Kernkomponenten

KRITIS-Kernkomponenten gab es bisher auch schon. Dazu zählten alle diejenigen Assets, die unmittelbar für den Betrieb der kritischen Anlagen notwendig waren oder deren Störung umgekehrt eine Störung der kritischen Dienstleistung bewirkt hätte.

Neu ist, dass für diese KRITIS-Kernkomponenten zukünftig explizit Mindeststandards durch das BSI definiert werden. Auch dürfen dafür zukünftig nur noch solche Komponenten von Herstellern verbaut werden, für die eine „Vertrauenswürdigkeitserklärung“ abgegeben wurde, die also demnach über ein BSI-Sicherheitskennzeichen verfügen. Diese Anforderung schließt die gesamte Zulieferkette des Herstellers ausdrücklich ein.

IT-Grundschutzprofil für Kommunen

Am 15. Oktober 2019 hat die Arbeitsgruppe „**Modernisierung IT-Grundschutz**“ mit der Unterstützung des Deutschen Städtetags, des Deutschen Landkreistags und des Deutschen Städte- und Gemeindebunds das IT-Grundschutzprofil in der überarbeiteten Version 2 vorgelegt. Bei der Neuauflage des Grundschutzpapiers wurde maßgeblich das IT-Grundschutz Kompendium in der Edition 2019 berücksichtigt.

Die Zielgruppe

Das IT-Grundschutz-Profil ist für Kommunalverwaltungen ausgelegt, die einen systematischen Einstieg in die Informationssicherheit suchen. Es ist adressiert an die Verantwortlichen in der Verwaltung, welche für die Umsetzung und Aufrechterhaltung der Informationssicherheit zuständig sind. Dies sind typischerweise die Hauptverwaltungsbeamtinnen und -beamten, welche die Ressourcen bereitstellen und das angestrebte Sicherheitsniveau einschließlich der Risiken verantworten, sowie die für die Steuerung und Koordination des Informationssicherheitsprozesses zuständigen Informationssicherheitsbeauftragten.

Zielsetzung

Dieses Profil basiert auf dem BSI-Standard 200-2 „IT-Grundschutz-Methodik“ und definiert die Mindestsicherheitsmaßnahmen, die in einer Kommunalverwaltung umzusetzen sind.

Das Profil erleichtert den Einstieg in die Informationssicherheit und hilft, die gröbsten Schwachstellen aufzudecken, die es zu beseitigen gilt, um möglichst schnell das Sicherheitsniveau in der Breite anzuheben. Um ein dem Stand der Technik angemessenes Sicherheitsniveau zu erreichen, müssen darauf aufbauend in einem weiteren Schritt zusätzliche Anforderungen erfüllt werden.

Die erheblichen Investitionen der Kommunalverwaltungen in der IT-Ausstattung müssen über angemessene Sicherheitsvorkehrungen geschützt werden. Das beschriebene IT-Grundschutzprofil umfasst die Mindestanforderungen, um hohe materielle und immaterielle Schäden (z. B. Rufschäden bzw. Vertrauensverlust) von Kommunalverwaltungen abzuwenden.

Schutzbedarf im höchsten Umfang

Serverräume sind Standorte von Daten, Netzwerkverbindungen und stellen der IT Infrastruktur die Anwendungen bereit. Hier treffen alle Anforderungen an Sicherheitsvorkehrungen zusammen.

Handlungsempfehlung

Die Anwendung des kommunalen IT-Grundschutz-Profils ist ein wichtiger Schritt beim Aufbau einer systematischen Informationssicherheit in den Kommunalverwaltungen.

Ziel muss es sein, darauf aufbauend mittelfristig ein Sicherheitskonzept gemäß der Standard-Absicherung (definiert in BSI-200-2) zu erstellen, da nur dies dem Schutzbedarf der Daten und Prozesse einer Kommunalverwaltung gerecht wird.

Darüber hinaus sind kritische Verfahrensbereiche und Verfahren, für die bereits eindeutige, rechtliche Vorgaben gelten (z. B. Waffenwesen oder Personenstandswesen), gemäß ihres höheren Schutzbedarfes mit zusätzlichen Maßnahmen abzusichern.

Rahmenbedingung

Eine Anwendung des Profils ist nur in Verbindung mit dem jeweils aktuellen IT-Grundschutz Kompendium des BSI möglich. Das Profil stellt eine Ergänzung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen [HR-ISLL-KV] dar, kann aber auch unabhängig davon genutzt werden. Die Handreichung beschreibt den Einstieg in Entwicklung und Gestaltung von Informationssicherheitsleitlinien (ISLL) sowie Wege zum Aufbau und Betrieb kommunaler Informationssicherheitsmanagementsysteme (ISMS).

Das vollständige Dokument wurde vom BSI unter der Adresse

https://.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.pdf

veröffentlicht.

Vorgehensweise nach IT-Grundschutz

Die aufgeführten Anforderungen sind Empfehlungen, die mindestens die Vorgaben der Basis-Absicherung des BSI-Standards 200-2 abdecken. Teilweise wurden zusätzlich zu erfüllende Standard-Anforderungen erweitert. Diese Ergänzungen sind notwendig, da Kommunalverwaltungen personenbezogene oder sonstige schützenswerte Informationen in teilweise öffentlich zugänglichen Räumlichkeiten verarbeiten.

Einführung ISMS beim Rhein-Kreis Neuss

Bei einem ISMS handelt es sich um die Verfahren und Regeln innerhalb eines Unternehmens, die dazu dienen, die Informationssicherheit zu definieren, dauerhaft zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Jede IT-Abteilung integriert Firewalls, analysiert Emails, schützt Server, Daten, betreibt Monitoring Systeme etc. Es gibt zahlreiche Regeln, Richtlinien und technische Vorgaben, die alle ihren wichtigen Teil zu einer möglichst vollumfassenden IT Sicherheit beitragen.

Alle dazu erforderlichen Maßnahmen müssen auch an Personalveränderungen, die ständige Weiterentwicklung von Technik und Prozessen angepasst und fortgeschrieben werden. Für die Erfassung der relevanten Informationen, Regeln und Maßnahmenkataloge wird die Einführung eines Informationssicherheits-Managementsystems (ISMS) empfohlen.

Die meisten Unternehmen führen Aktivitäten im Bereich Informationssicherheit durch, häufig geschieht dies jedoch ohne eine prozessorientierte Koordination. Das kann folgende Auswirkungen haben:

- fehlende Ausrichtung der Informationssicherheit an Geschäftsprozesse bzw. der Wertschöpfungskette
- redundante Planung von Sicherheitskonzepten
- ähnliche Aktivitäten im Unternehmen zur Herstellung von Informationssicherheit mit unterschiedlichen Ansätzen.

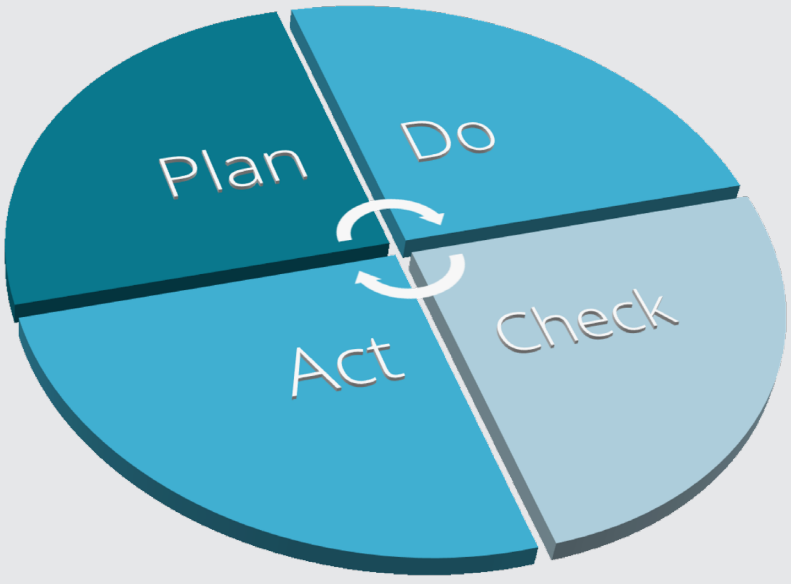
Allgemein wird heute ein definierter Prozess für die Einrichtung, für die Umsetzung, Überwachung, Überprüfung, Aufrechterhaltung und Verbesserung der Informationssicherheit gefordert. Die wesentliche Zielsetzung dabei ist, die Risiken in der Informationssicherheit besser zu erkennen und zu beherrschen. Durch die strukturierte Vorgehensweise und Methodik zur kontinuierlichen Bearbeitung bzw. Verbesserung der Informationssicherheit wird diese planbar und angemessen effizient und aktuell.

Der Rhein-Kreis Neuss beginnt im Januar 2020 mit der Überarbeitung der vorhandenen Regelwerke und der Übertragung seiner Sicherheitsvorgaben in ein Informationssicherheits-Managementsystem. Dabei wird das ISMS zahlreiche Prozesse mit IT-Bezug betreffen, zu denen eine fortwährende Verbesserung Der IT-Sicherheitsregeln erforderlich ist. Empfohlen ist hierzu der Aufbau nach der Grundlage des „PDCA Modells“.

Das PDCA-Prinzip

Ein geeignetes Prozessmodell für die kontinuierliche Verbesserung eines ISMS ist das PDCA-Modell (PDCA Plan, Do, Check, Act). Dieses Modell lässt sich auf nahezu alle Managementsysteme anwenden und wird benutzt, um die ISMS-Prozesse zu strukturieren.

Auf der Grundlage des PDCA-Modells wird der Status Quo des ISMS Regelwerks permanent in Frage gestellt und soll in einem wiederkehrenden Regelkreis Verbesserungen an Abläufen und Prozessen starten.



ISMS Prozessablauf nach dem PDCA Modell

Die erste Phase (Plan) beinhaltet die Planung und Organisation des ISMS und der jeweiligen Schutzmaßnahmen. Typische Fragestellungen sind z.B.:

- Welche Ziele sollen in der Informationssicherheit erreicht werden?
- Welche Ressourcen und Verantwortlichkeiten gibt es?
- Welche Prozesse werden festgelegt, um die Schutzziele zu erreichen?
- Welcher Schutzbedarf besteht und wie wird dieser analysiert?
- Wie werden Risiken erkannt und in Kennzahlen umgesetzt?
- Wie erfolgt der Umgang mit Risiken?
- Welche Schutzmaßnahmen werden wie und durch wen eingeführt?

In der zweiten Phase (Do) werden die ISMS-Prozesse und Schutzmaßnahmen eingeführt und umgesetzt. Die Leitfragen hierbei lauten:

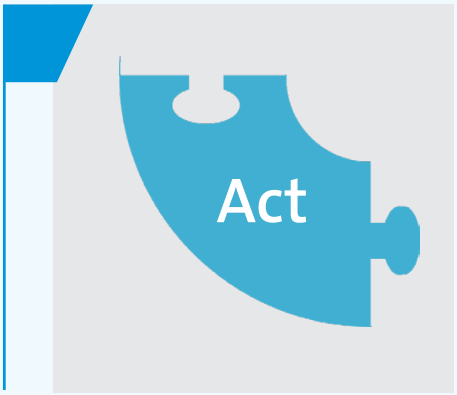
- Werden die ISMS-Prozesse gemäß ihrer Festlegung implementiert?
- Wird die Einführung der Schutzmaßnahmen geplant, durchgeführt und kontrolliert?
- Werden die Informationen klassifiziert und in die ISMS-Prozesse und Dokumente eingebracht?

In der dritten Phase (Check) sind implementierte Schutzmaßnahmen im laufenden Betrieb zu überwachen und hinsichtlich Effizienz und Aktualität zu überprüfen:

- Werden organisatorische und technische Audits durchgeführt?
- Wie hoch ist der Sensibilisierungsgrad?
- Werden das Umfeld und Sicherheitsvorfälle überwacht?
- Werden Notfall- bzw. Business-Continuity-Pläne getestet?
- Wie wird die Informationssicherheit gemessen?
- Prüft das Management die Ergebnisse und wie werden Entscheidungen getroffen?

Durch die vierte Phase (Act) kann die Sicherheit der implementierten Schutzmaßnahmen und der Informationssicherheitsprozess verbessert bzw. optimiert werden. Die Fragestellungen sind dabei:

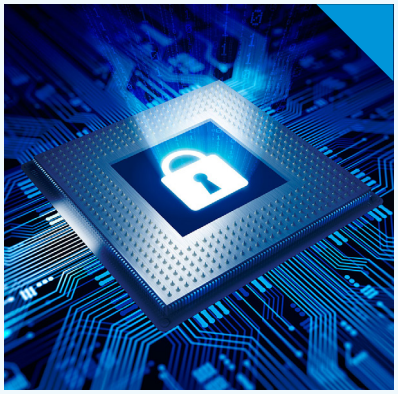
- Wie und wann werden die Informationssicherheit und das ISMS verbessert?
- Werden Changes im ISMS berücksichtigt?
- Ist das ISMS in einem Handbuch beschrieben?



Einführung und Betrieb eines ISMS

Die Einführung des Informationssicherheit-Managementsystems ist eine strategische Entscheidung für die Kreisverwaltung. Seine Gestaltung und Umsetzung hängen von den Bedürfnissen und Zielen, Sicherheitsanforderungen, eingesetzten Verfahren sowie der IT Strukturen vor Ort ab.

Auch Kommunalverwaltungen bekommen mit einem ISMS ein Werkzeug an die Hand, das es ihnen ermöglicht, ihre IT-Sicherheit strukturiert zu bewerten und kontinuierlich zu verbessern.



Aus den vier Phasen mit den entsprechenden Leitfragen ergeben sich im Informationssicherheitsprozess konkrete ISMS-Prozess-schritte für die Umsetzung der Informationssicherheit.

Im Rahmen der Zusamenarbeit werden der Rhein-Kreis Neuss, die Städte Dormagen, Grevenbroich, Kaarst und Meerbusch im 1. Quartal 2020 in einem gemeinsamen Workshop die Basisdaten für das ISMS aufbauen.

Der Rhein-Kreis Neuss erwartet durch die Beteiligung der Kommunen einen gegenseitigen Mehrwert. Die ISMS-Strukturdaten lassen sich an vielen Stellen austauschen.

Kaffee geholt. Daten weg.

Sperren Sie den PC auch bei kurzer Abwesenheit!

Der Schutzbedarf beim Emailverkehr

Die Spam-E-Mail ist für Angreifer weiterhin das beliebteste Mittel, um auf fremde Systeme und Unternehmensnetzwerke zu gelangen. Im September 2019 lag der Anteil der Spam-Mails am gesamten E-Mail-Verkehr weltweit bei rund 54,7 Prozent.

Alle unerwünscht zugesandten E-Mails werden generell als Spam bezeichnet. Diese lassen sich grob in drei Formen unterteilen:

- **Klassischer Spam** wird häufig für Produkt-, Wertpapier- oder Dienstleistungswerbung benutzt und zudem für Betrugsversuche wie Vorschussbetrug eingesetzt. Beim Vorschussbetrug soll das Opfer z. B. dazu animiert werden, Geld für eine Dienstleistung oder Ware vorab zu überweisen, die später nicht geliefert wird.

- Mit sog. **Schadprogramm-Spam** (Malware-Spam) wollen Angreifer Systeme der Empfänger mit Schadprogrammen infizieren. Dies kann direkt durch ein Schadprogramm im E-Mail-Anhang oder indirekt durch einen Link im E-Mail-Text oder im Anhang erfolgen, der auf ein Schadprogramm verweist.

- Mit **Phishing-Nachrichten** werden Benutzer dazu bewogen, ihre Zugangsdaten (z. B. zu Internet-Banking, Bezahldiensten, sozialen Netzwerken, Einkaufsportalen etc.) auf Webseiten unter der Kontrolle der Angreifer einzugeben.

Der Spam-Versand erfolgt in den meisten Fällen entweder über kompromittierte Server, infizierte Client-Systeme oder mithilfe ausgespähter Zugangsdaten über legitime E-Mail-Konten. Häufig sind die Spam versendenden Systeme zu einem Botnetz zusammengeschlossen.

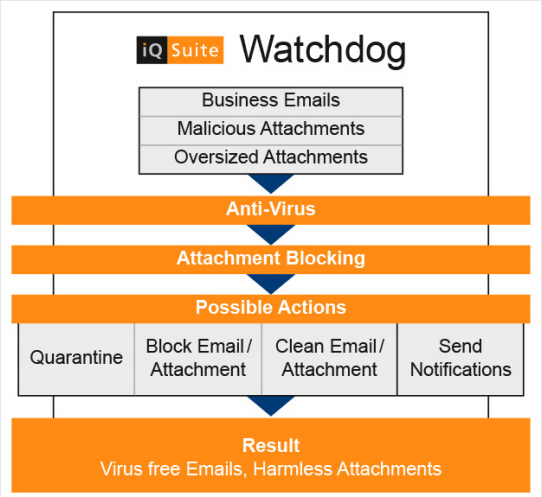
Die versendeten Anhänge werden stetig angepasst, um die Erkennung durch Antiviren-Software zu unterlaufen. Anfang April 2019 wurden z. B. Dokumente als verschlüsselte ZIP-Dateien versendet und das Passwort in der E-Mail genannt. Der fingierte Inhalt der E-Mail war häufig in gutem Deutsch verfasst und sollte dem Adressaten eine dringende Angelegenheit suggerieren (Rechnung, Auftragsbestätigung etc.).

Über Emotet hinaus wurden auch weitere kleine Wellen beobachtet. Hervorzuheben ist der Versand von RTF- und teilweise auch MS-Word-Dokumenten, die die MS-Equation-Schwachstelle (CVE-2017-11882) ausgenutzt haben.

Ein weiterer Trend ist der Versand von MS-Office-Dokumenten, die keinen Schadcode enthalten, diesen jedoch über MS-Office-Mechanismen nach dem Öffnen des Anhangs aus dem Internet nachladen.

Die Zustellung einer Email an den Rhein-Kreis Neuss durchläuft mehrere Prüfroutinen beim Rechenzentrum, anschließend weitere Softwareprüfungen bei der Kreisverwaltung (siehe Seite 15).

Sicherheitskonzept Email beim Rhein-Kreis Neuss



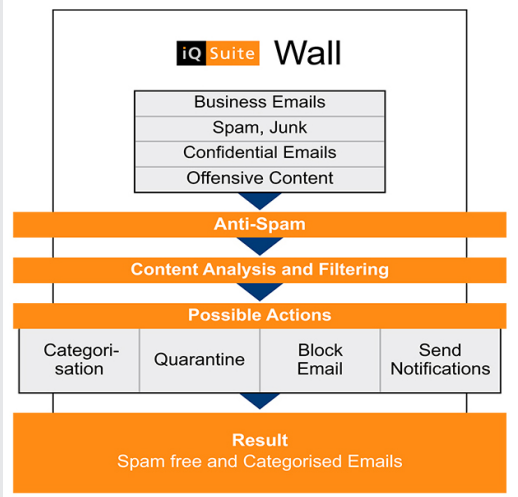
Die Anforderungen gegen Malware

Zum Schutz gegen schadhafte Auswirkungen durch Emailinhalte ist ein abgestuftes Sicherheitskonzept erforderlich:

- Viren und Trojaner müssen zuverlässig erkannt werden.
- Unterschiedlichste Dateiformate müssen manipulationssicher analysiert werden.
- Unternehmensspezifische Richtlinien müssen den Umgang mit Dateianhängen steuern.
- Java Script Code und Weblinks in Anhängen müssen erkannt und entfernt werden.
- Dateieinschränkungen müssen auch auf komprimierte Dateiarchive angewandt werden.

Email Report Dezember 2019

Emails an den Rhein-Kreis Neuss	**1.100.000**
Bedrohungen:	**95,4%**
Virenfreie Mails:	**4,6%**



Maßnahmen gegen Spam Mails

Ein weiterer Bestandteil zur Prüfung des Emailverkehrs ist eine umfassende Gesamtlösung zum Spamschutz und zur Inhaltsanalyse. Hierzu sind durch den zentralen Spamschutz mehrere Bedingungen zu erfüllen:

- Die Kombination unterschiedlicher Analyseverfahren für eine möglichste hohe Spam-Erkennungsrate.
- Automatisierte Black-/Whitelists müssen mit einer leistungsfähigen Textanalyse- und Klassifizierungstechnologie kombiniert werden.
- Eine selbstlernende E-Mail-Analyse (CORE - Content Recognition Engine) unterstützt dabei nicht nur den Schutz vor Spam, sondern ist auch Basis für eine komfortable Autoklassifizierung von E-Mails.
- Die Prüfung muss gemäß der Unternehmensrichtlinien auf verbotene, nicht erwünschte oder vertrauliche Inhalte erfolgen.
- Flexible Benachrichtigungen über geblockte E-Mails an Administration oder Empfänger/-Absender müssen generiert werden.

Endpoint Protection beim Rhein-Kreis Neuss

Der Schutz eines Rechners oder Servers umfasst heutzutage mehr wie ein Antivirenprogramm. Es bedarf einer Softwarelösung, die Laptops, Desktops und Server gegen Malware, Risiken und Sicherheitslücken schützt.

Es ist schon einige Zeit her, dass die Anbieter ihre Software für den PC Schutz als Antivirensoftware beworben haben. Heute ist ein erweiterter Systemschutz erforderlich, um proaktiv gegen bekannte und unbekannte Bedrohungen wie Viren, Würmer, Trojanische Pferde und Adware abzusichern. Inzwischen gibt es Angriffe, die herkömmliche Sicherheitsmaßnahmen umgehen, wie z. B. Rootkits, neuartige Schadprogramme und mutierende Spyware.

Ein vollumfänglicher Schutz muss verschiedene Erkennungs- und Behebungsmechanismen für persistente Bedrohungen mithilfe hochmoderner Angriffsanalytik beinhalten und den Diebstahl von AD-Zugangsdaten verhindern.

Infizierte Geräte haben schwerwiegende Störungen des Geschäftsbetriebs zur Folge. Eine innovative Angriffsabwehr und die Reduktion der Angriffsfläche müssen einen leistungsstarken Schutz während des gesamten Angriffslebenszyklus gewährleisten.

Administratoren brauchen außerdem eine Management Suite, um ein Regelwerk für alle Sicherheitsrisiken, aber auch notwendige Ausnahmen aufgrund einer überbewerteten Blockierung von Anwendungen zu verwalten. Die IT Abteilung muss zudem umgehend informiert sein, sofern Angriffe und Gefahren erkannt und ein sofortiges Eingreifen der Administration erforderlich wird.

Alle dafür notwendigen Produkte sind seit vielen Jahren Bestandteil des Bedrohungsschutzes beim Rhein-Kreis Neuss. Auch hier ist eine ständige Marktsichtung erforderlich, um alle notwendigen Erkennungsmethoden im Bereich Computing als auch den Schutz der zentralen Datenspeicher sicherzustellen.

Der Rhein-Kreis Neuss setzt zum Endpoint Management Produkte der Firma Symantec ein. Symantec hat das Firmenkundengeschäft an den Chiphersteller Broadcom verkauft. Der Ankauf der Produkte soll das Infrastruktur-Geschäft von Broadcom stärken, zu dem auch der Software-Riese CA Technologies zählt.

Abhängig von der Softwareentwicklung der Endpoint Security von Symantec kann ein Produktwechsel erforderlich werden.

Schutz für alle Phasen des Angriffslebenszyklus

Pre-Attack

Reduktion der Angriffsfläche

- Vulnerability Remediation
- Breach Assessment
- Device Control
- App Isolation & App Control

Attack

Angriffsprävention

- Malware Prevention
- Exploit Prevention
- Intensive Protection
- Network Connection Security

Breach

Prävention von Übergriffen

- Intrusion Prevention & Firewall
- Deception
- Active Directory Security
- Auto-Managed Policies

Post Breach

Reaktion und Behebung

- Targeted Attack Analytics
- Threat Hunting
- Integrated Response
- Expert SOC Investigator

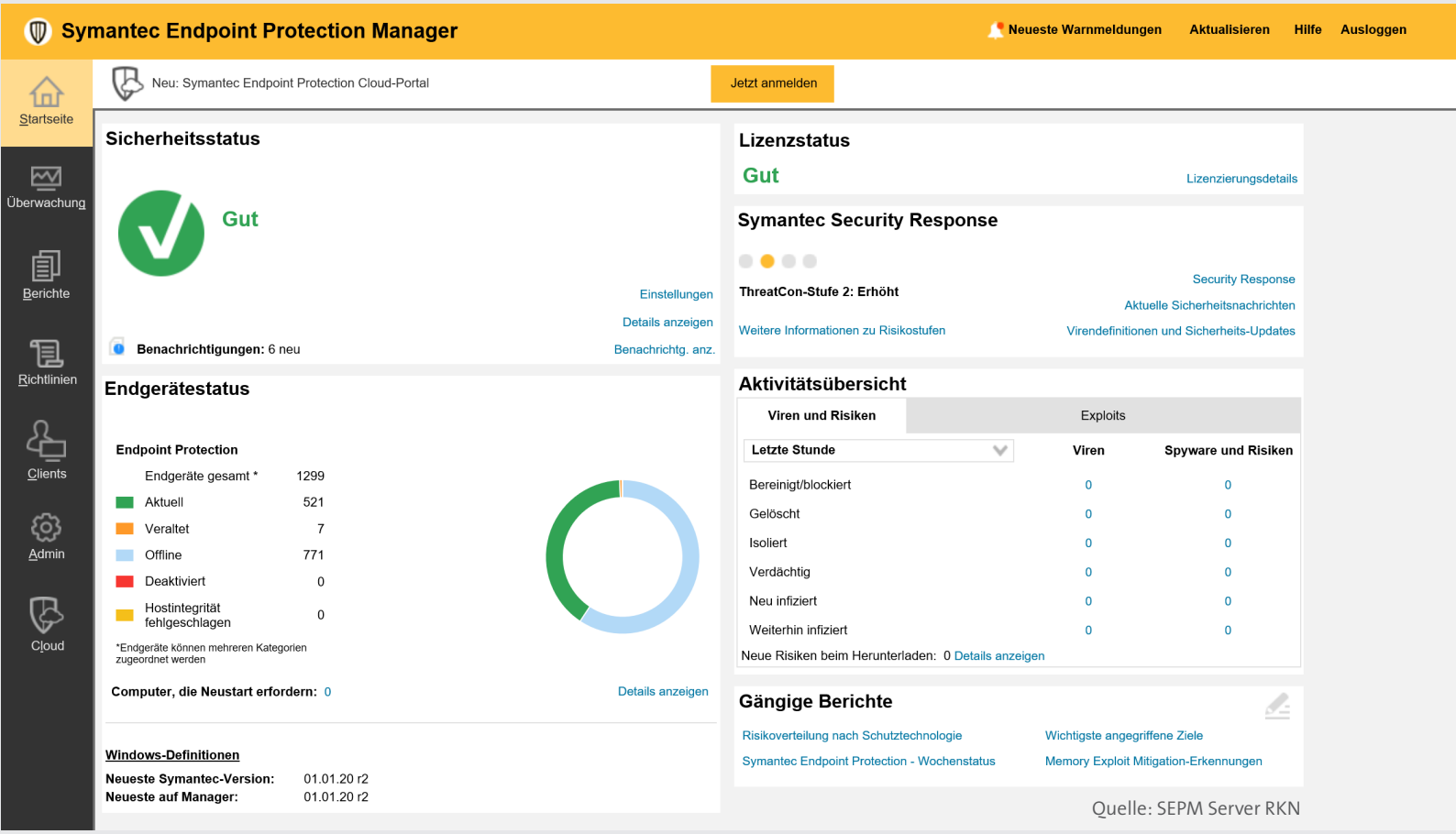
Quelle: Symantec

Prävention im gesamten Cyber Attack Lifecycle

Alle Angriffe bestehen aus mehreren aneinandergereihten Stufen, die den **Angriffslebenszyklus** bilden. Die vier wichtigsten Phasen, in denen Angriffe verhindert werden können sind: Lieferung, Ausnutzung der Schwachstelle, Installation der Malware sowie Steuerung & Kontrolle.

Geräteverwaltung, Richtlinien, Alarme

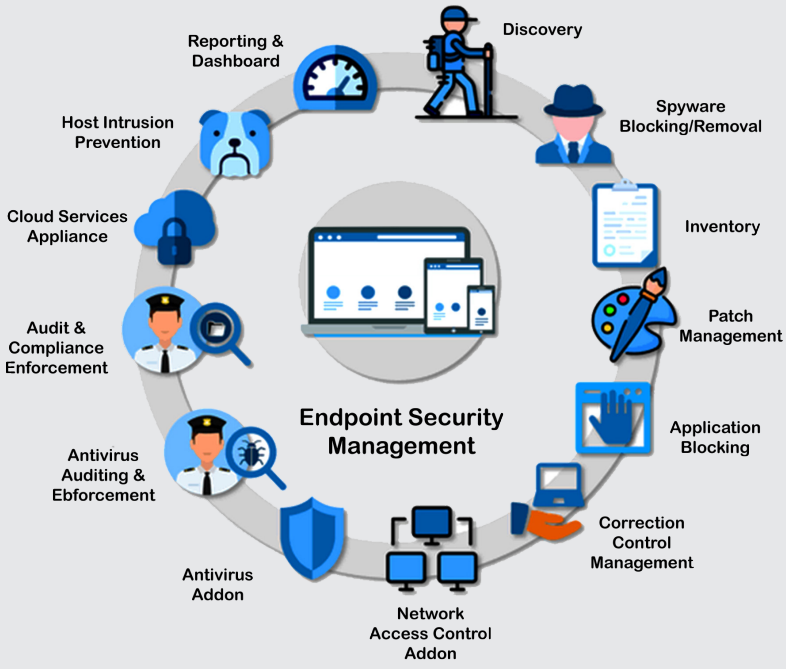
Alle renommierten Anbieter von Schutzsoftware bieten Komponenten für eine serverbasierte Administration der schutzbedüftigen IT Ressourcen im Unternehmen an. Auch beim Rhein-Kreis Neuss gelten geregelte Schutzvorgaben.



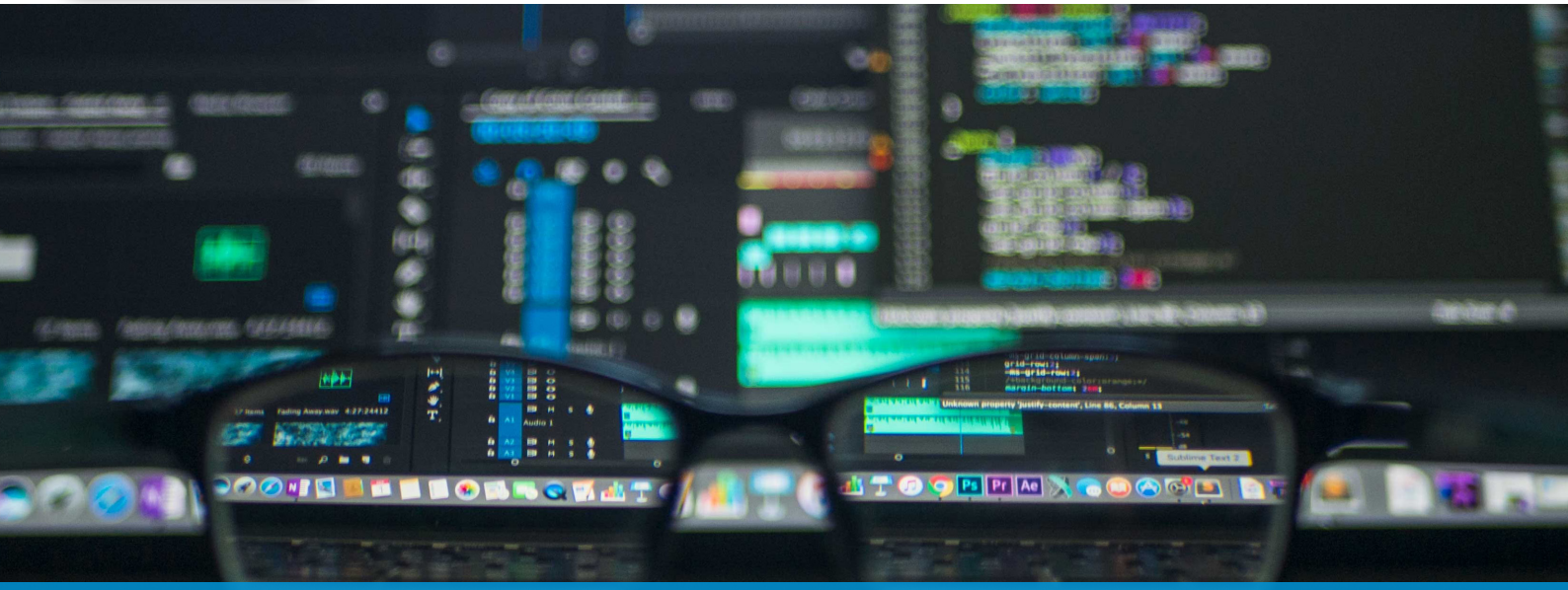
Quelle: SEPM Server RKN

Funtionsumfang

für ein vollumfängliches Endpoint Security Management



Quelle: Sketch Bubble



Endpoint Detection & Response (EDR)

Auch Behörden müssen heute umfassend über die Vorgänge in ihrem Netzwerk informiert sein. Nur so lassen sich Angriffe von außen, interne Sicherheitslücken oder Fehlverhalten von Mitarbeiter/Innen identifizieren. EDR-Tools unterstützen bei der Arbeit.

Alle Verwaltungen mit IT Infrastrukturen stehen unter Dauerbeschuss von Cyberkriminellen und Hackern. Diesem Druck zu widerstehen und gleichzeitig ein performantes Netzwerk zu garantieren, ist leichter gesagt als getan. Denn die Security-Grundausstattung mit Antiviren-Lösungen und Endpoint Protection reicht oft nicht nicht mehr aus.

Hacker und Cyberkriminelle planen gut getarnte Angriffe, die nur sehr schwer an einzelnen Verhaltensauffälligkeiten auf den Rechnern sicher zu identifizieren sind. Für viele Administratoren bietet sich inzwischen der Einsatz zusätzlicher Softwareprodukte zur Erhöhung der Gefahrerkennung an.

Mit Endpoint Detection and Response (EDR)-Lösungen lassen sich softwaregesteuert verdächtiges Verhalten und Sicherheitslücken im Netzwerk automatisch aufspüren. Alle Aktivitäten innerhalb der IT-Infrastruktur (Nutzer-, Datei-, Prozess-, Registry-, Speicher- und Netzwerkvorgänge) können in Echtzeit überwacht und bewertet werden, sodass bei Bedarf sofort gehandelt werden kann. Auf diese Weise lassen sich erste Spuren von Hackern identifizieren, Fehlverhalten der Mitarbeiter bestimmen und Sicherheitslücken ausfindig machen.

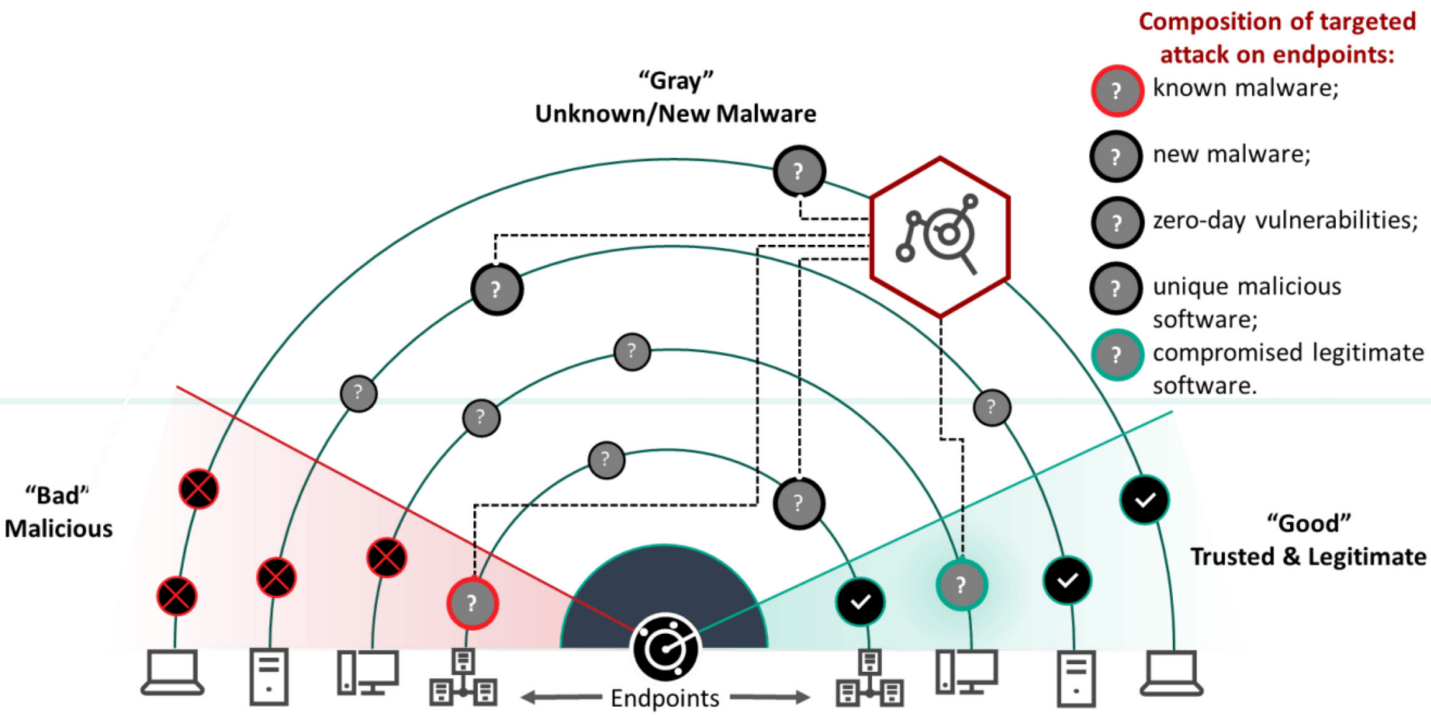
Die Auswertung der gesamten Endpoint-Daten in einem Unternehmen lässt Rückschlüsse auf die Validität einzelner Abläufe zu. Eine genaue Erfassung von alltäglichen Vorgängen wie dem Kopieren von Dateien, User Zugriffen auf bestimmte Bereiche im Netzwerk oder aber auch An- und Abmeldungen von Anwendern erlauben bei entsprechender Auswertung ein Herausfiltern bösartiger Aktivitäten.

EDR-Lösungen ersetzen dabei keine Endpoint Protection oder Antiviren-Lösungen, sondern ergänzen sie um die Erkennung von Verhaltensanomalien, die im Unternehmensnetzwerk und auch auf den Endpoints auftreten. Die Erkennung basiert auf vordefinierten Regeln, die alle legalen Aktivitäten abbilden. Basierend auf diesen Angaben analysiert die EDR-Anwendung die Datenströme.

Inzwischen haben fast alle Anbieter von Sicherheitslösungen EDR-Technologie in ihrem Software Portfolio. Aufgrund der Vielschichtigkeit und der Komplexität der Materie kamen EDR-Lösungen bislang lediglich in Großkonzernen zum Einsatz, bei denen die IT-Abteilungen entsprechende Ressourcen und Knowhow mitbringen. Inzwischen haben auch immer mehr mittelständische Unternehmen die Möglichkeit und auch Notwendigkeit, EDR in ihren Netzen einzusetzen. Der Rhein-Kreis Neuss beschäftigt sich in 2020 ebenfalls mit den angebotenen EDR Produkten.

EDR in der Praxis

Beispiel Fa. Kaspersky: Analyse eines Datenverkehrs und Einstufung des Risikos



Leistungsmerkmale eines EDR Systems

1 **„Echtzeit"-Analyse:** Ein EDR System kann fortlaufend Dateien analysieren, um zeitaufwändige regelmäßige Scans überflüssig zu machen.

2 **Keine Signaturen erforderlich:** Die Bedrohungsanalyse ist nicht auf tägliche Definitionsupdates angewiesen.

3 **Machine Learning:** Das System setzt maschinelles Lernen ein, um die geeignetsten Reaktionen auf Bedrohungen zu bestimmen.

4 **Autogenerierte Warnungen:** Warnmeldungen, werden erstellt, wenn eine Bedrohung entdeckt oder neutralisiert wird.

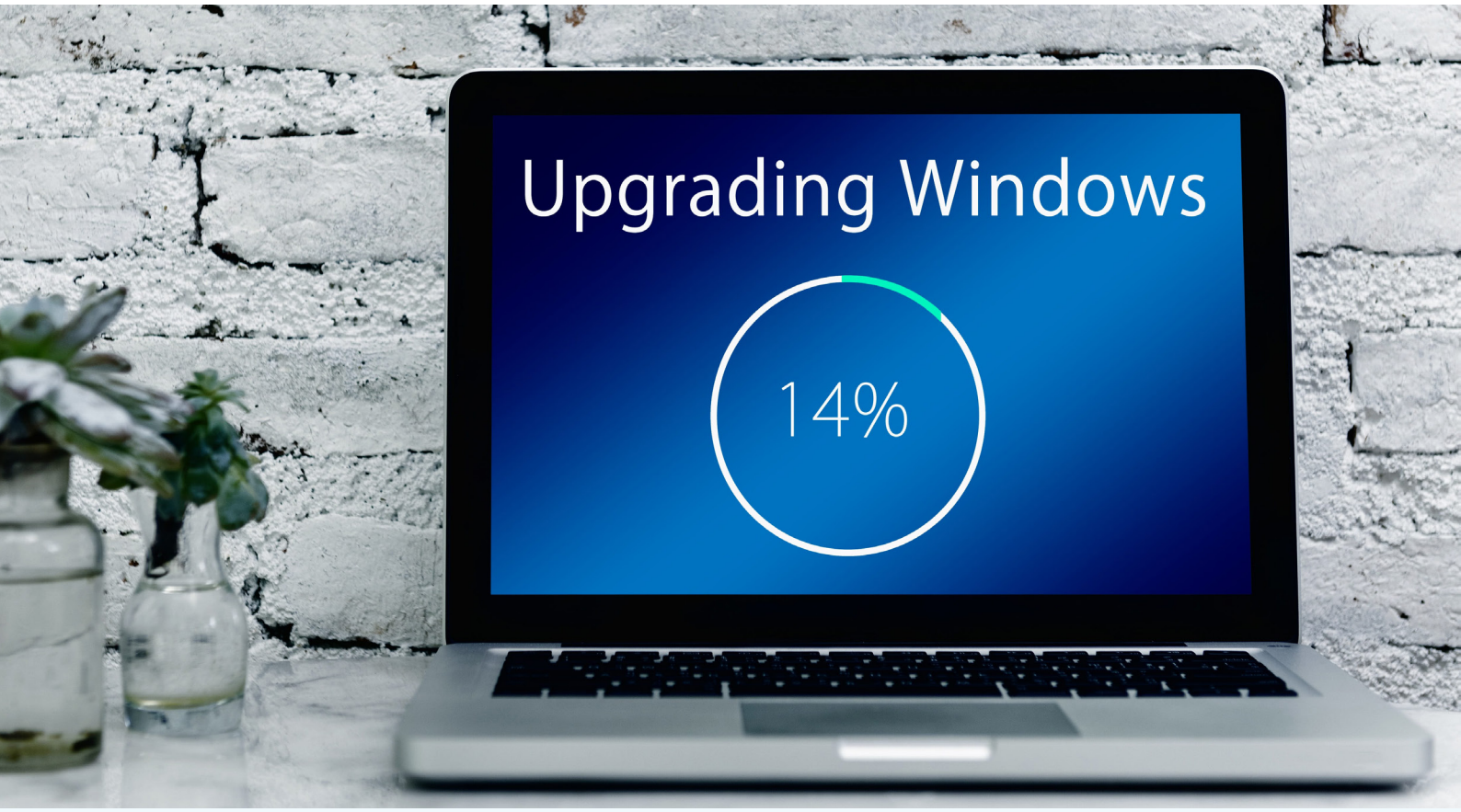
5 **Bedrohungsstatistik:** Zusammengefasste Daten zu Bedrohungen sind im Zeitverlauf ersichtlich. Der aktuelle Bedrohungsgrad kann eingeschätzt werden.

6 **Forensik:** Eine Übersicht über den Ablauf eines Angriffs lässt Angriffsmuster erkennen und verstehen.

7 **Richtlinien:** Ein Richtlinien-basierter Schutz kann individuell angepasst werden. Der Datenverkehr am Endpunkt kann detailliert festgelegt werden.

8 **Verbesserte Quarantäne:** Netzwerkverbindungen können ad hoc getrennt werden, um die Verbreitung einer Bedrohung zu unterbinden.

Automatisches Schwachstellenmanagement



Im Mai 2017 gab es den bislang größten Angriff durch Ransomware. „WannaCry“ befiel damals Schwachstellen in Windows Betriebssystemen und verschlüsselte Daten. Eine Wiederherstellung der Daten war nur gegen Zahlung von Lösegeldern in der Kryptowährung Bitcoin möglich.

Viele Unternehmen wurden durch die WannaCry Attacke lahmgelegt und für alle Betroffenen galt die gleiche Ursache: Es wurden bekannte Schwachstellen im Betriebssystem ausgenutzt. Solche Schwachstellen im Software Code bleiben oft über längere Zeit unentdeckt, aber mit ihrer Identifizierung werden sie zu einem großen Risiko. Ein Angriff ist dann mit einfachen Mitteln möglich.

Im Internet kursieren Exploits zu unzähligen Schwachstellen. Befallen werden häufig ältere Windows-Betriebssystemversionen, die nicht über die neuesten Patches verfügen. Um Sicherheitslücken zuverlässig aufzuspüren, müssen nicht nur Betriebssystem und Anwendungen ständig gepatcht werden, Administratoren müssen sich außerdem in regelmäßigen Abständen über neu veröffentlichte Lücken und Patches informieren.

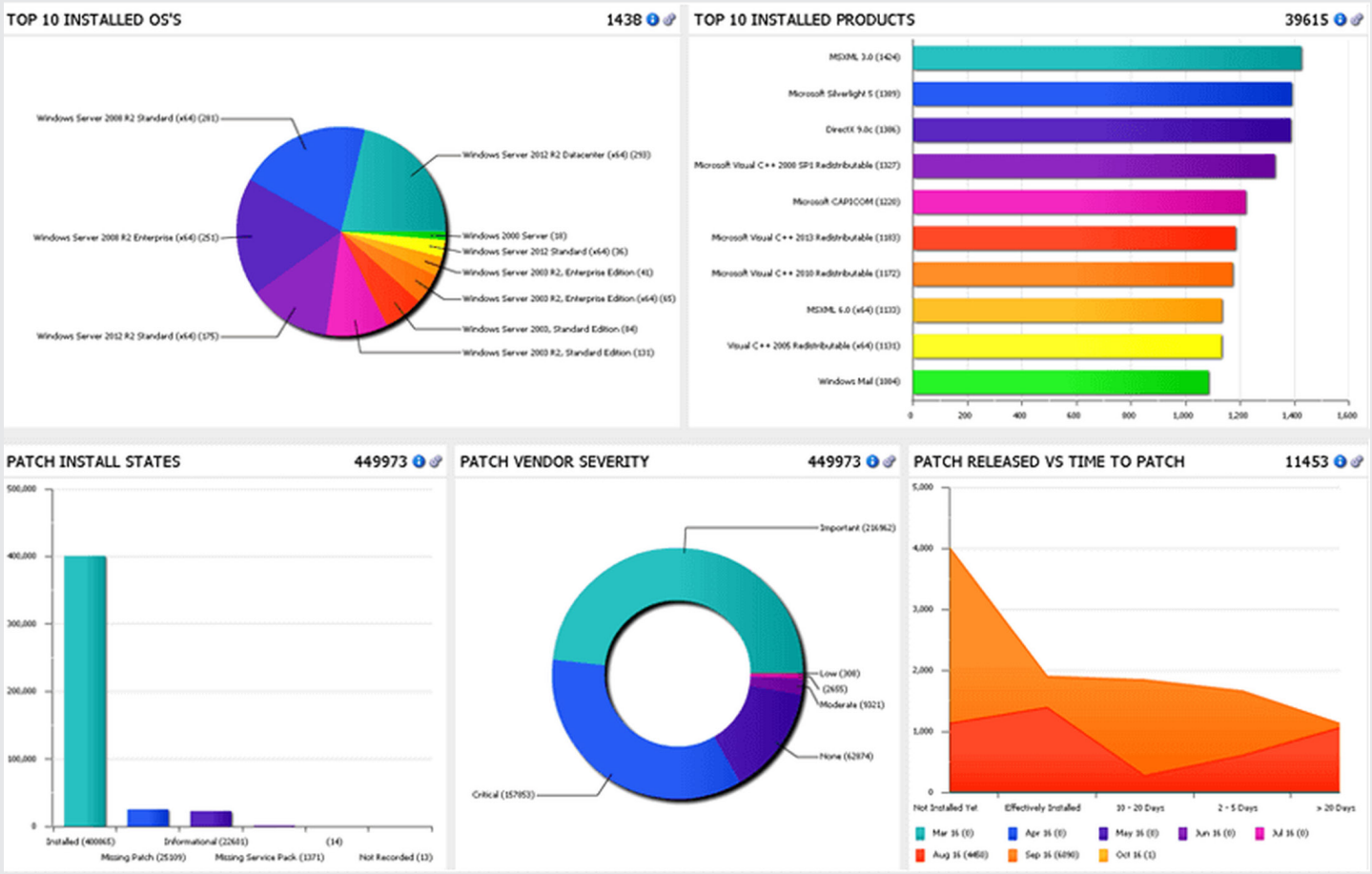
Ohne geeignete Hilfsmittel ist dieser Prozess in der Praxis bei der hohen und ständig wachsenden Anzahl der Sicherheitslücken manuell nicht mehr zu bewerkstelligen.

Eine Abhilfe schafft ein automatisiertes Schwachstellenmanagement. Sind mögliche Schwachstellen identifiziert, lassen sie sich mit einem Patch-Manager beheben. Administratoren können damit Sicherheitslücken schließen, Fehler korrigieren und Funktionen erweitern.

Durch die regelbasierte Freigabe von Patches können diese Maßnahmen unternehmensweit implementiert werden, ohne dass sich Systemverantwortliche manuell um jeden einzelnen PC oder Server kümmern müssen.

Die wesentlichen Kernfunktionen

Ein Schwachstellenmanagement hilft dabei, den Überblick über die Infrastruktur zu behalten und die Produktivität der Endbenutzer abzusichern.



Quelle: Ivanti Asset Manager / Endpoint Manager

- Mit einer Patch-Lösung lassen sich Betriebssysteme und viele verwendete Applikationen aktualisieren.
- Virtuelle Infrastrukturen, in der Regel im Serverumfeld, lassen sich zenral aktualisieren.
- Je nach Konfiguration können fehlende Patches in der gesamten Organisation verteilt werden.
- Durch agentenloses Patching ist keine Remote Installation erfroderlich.
- Automatisierungs- und Reporting-Funktionen sind Bestandteil einer Patch-Management Lösung.

Status beim Rhein-Kreis Neuss

Automation für alle Windows 10 Clients ist im Einsatz.

Nächstes Ziel

Verbesserung der Patchverteilung für die zunehmende Zahl an Serversystemen.

Passwörter und Dark Web Analyse

Das beliebteste Passwort der IT Nutzer in Deutschland ist immer noch "**123456**". Einige weitere schwache und unsichere Zahlenreihen landen ebenfalls in den aktuellen Top Ten, die das Hasso-Plattner-Institut (HPI) anhand geleakter Zugangsdaten ermittelt hat.

Insbesondere IT Abteilungen verwalten für ihre zahlreichen administrativen Aufgaben beim Umgang mit Hard- und Software viele bedeutende Kennwörter. Daraus ergibt sich eine besondere Verantwortung für einen restriktiven und speziell gesicherten Umgang von systemrelevanten Passwörtern.

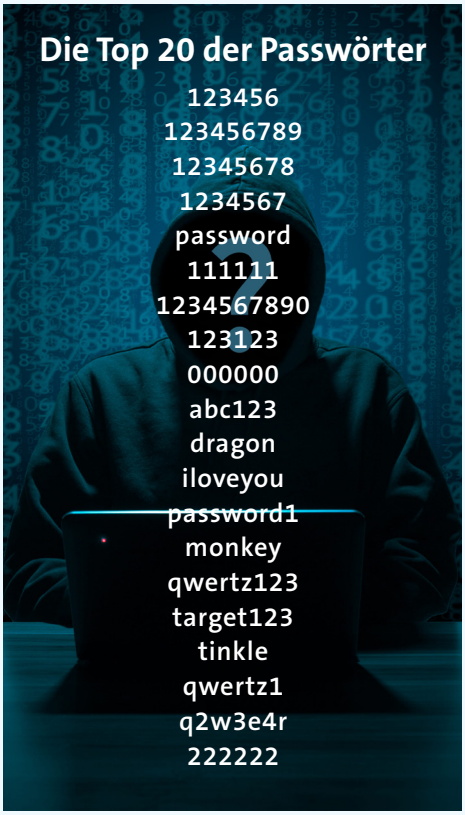
Auch für eine sichere IT Administration ist es unabdingbar, sensible Login Informationen gemeinsam zu verwalten. Der Rhein-Kreis Neuss setzt hierzu in der IT Abteilung eine spezielle Passwort Datenbank mit einem Rollen basierten Zugriffskonzept für zentral erforderliche Zugangsdaten ein.

Für alle Beschäftigten des Rhein-Kreises Neuss gelten die Vorgaben zur Verwendung sicherer und komplexer Kennwörter. Alle Beschäftigten müssen sensibilisiert sein, mit ihren Kennwörter vertrauensvoll und verantwortungsbewusst umzugehen.

Seit 2019 führt der Rhein-Kreis Neuss regelmäßig eine Dark Web Analyse zu allen Login Daten in Bezug auf die Domain rhein-kreis-neuss.de durch. Durch ein spezielles Programm wird geprüft, ob zu Emailadressen mit der Endung @rhein-kreis-neuss.de im Darknet Zugangsdaten veröffentlicht sind.

Dieses Problem kann unter anderem dann auftreten, wenn die Kundendatenbanken von Unternehmen gehackt und die Inhalte veröffentlicht werden. Im Jahr 2013 wurden z.B. nach einem bekannt gewordenen Einbruch ins Adobe Netzwerk die Daten von mindestens 38 Millionen Kundenkonten kompromittiert.

Sofern im Ergebnis einer Dark Web Analyse ein offengelegter Account des Rhein-Kreises Neuss enthalten ist wird die betroffene Person umgehend informiert, um eine sofortige Änderung der auffälligen Zugangsdaten durchzuführen.



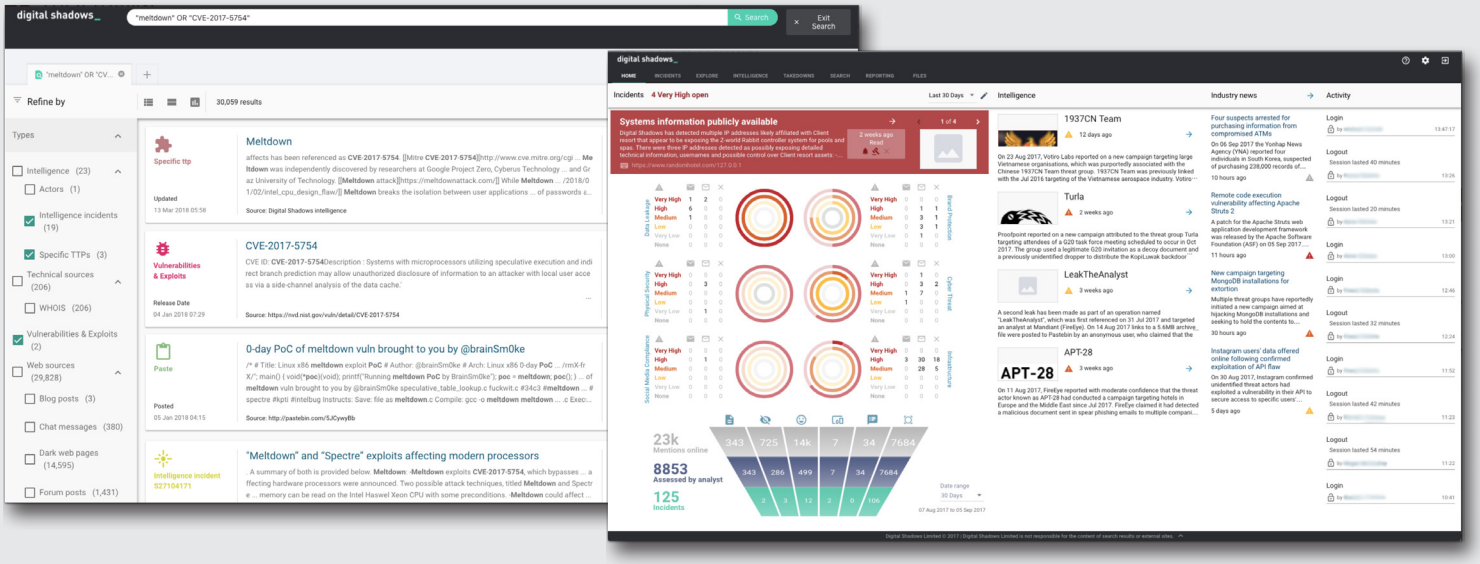
Dark Web Analyse der Kreisverwaltung

Beispiel eines beauftragten Berichts

+ Periodische Berichte werden beauftragt, keine eigenen Ressourcen erforderlich

- Keine tagesaktuellen Ergebnisse, kein Einfluss auf Berichtsparameter

Optional: Analyse mit Echtzeitdaten



+ Sicherheitsanalysen, Bewertungen, Threat Intelligence Reports in tagesaktueller Auswertung

- Manuelle Auswertung erforderlich, eigene Risikoabschätzung, personeller Aufwand

Das persönliche IT-Sicherheitsbewusstsein

Die Bedrohungslandschaft der Cyber Kriminalität ändert sich ständig. Die Konstante Mensch muss sich deshalb häufig darauf anpassen, wie ein vertraulicher und sicherer Umgang mit den Daten, Zugangsdaten usw. möglich bleiben.

Zahlreiche Schadensereignisse werden nicht durch Schadcode oder Malware erzeugt, sondern haben ihre Ursache im Verhalten der Mitarbeiter/Innen. Vor allem Angriffe mit Ransomware und Phishing-Methoden stellen ein großes Problem für Unternehmen dar, weil sie sich die mangelnde Erkennung einer Cyber Gefahr durch die Mitarbeiter/Innen zunutze machen.

Oftmals genügt schon ein einziger unaufmerksamer Beschäftigter, um die komplette Unternehmens-IT in Mitleidenschaft zu ziehen. Der unbedachte Klick auf einen Link, das sorglose Öffnen eines E-Mail-Anhangs, das Installieren unautorisierter Software oder das Mitbringen eigener Hardware können bedeutenden Schaden auslösen.

Awareness Strategie

Alle Mitarbeiter/innen sollen zukünftig verstärkt im eigenen Sicherheitsbewusstsein geschult und trainiert sein. Es muss geprüft werden, welche Maßnahmen Wirkung zeigen und wie langfristige Schulungserfolge erzielt werden. Für die Sensibilisierung können unterschiedliche Informationen genutzt werden:

- Kurzvideos
- Präsenzschulungen
- E-Learning
- Aktuelle Tagesnachrichten

Um ein besseres Bewusstsein für IT Sicherheit zu schaffen und die Verhaltensweisen nachhaltig zu ändern benötigt man mehr als eine einmalige Maßnahme, vielmehr handelt es sich um einen kontinuierlichen Lernprozess.

Funktionsmodell von Online-Trainingsplattformen: Das vorhandene Wissen feststellen, Neues lernen, Üben, Prüfen – und das Ganze nochmal von vorn. (Quelle: Kaspersky)

Online Training

Immer mehr Unternehmen nutzen Online-Trainingsplattformen. Darin integriert sind Trainingsmodule zu allen relevanten Bereichen der IT-Sicherheit, untern anderem zu den Themen sicheres Surfen, E-Mail-Sicherheit und Datenschutz. Die Lektionen sind auf die Bedürfnisse der einzelnen Nutzergruppen zugeschnitten.

Die Mitarbeiter/Innen müssen innerhalb festgelegter Zeiträume die Lektionen lernen und Tests darüber ablegen. Bei simulierten Phishing-Angriffen können sie dann beweisen, wie gut sie die Lektionen verinnerlicht haben und nicht auf Betrugsversuche reinfallen.

Das Verhalten der Mitarbeiter im Auge behalten

Praktisch alle diese Lernplattformen sind nach dem Prinzip „**Assess – Educate – Reinforce – Measure**“ aufgebaut. Am Anfang steht die Feststellung des aktuellen Wissenstands, dann kommt der auf den Anwender zugeschnittene Unterricht, das „Festsetzen“ des erlernten Stoffs durch praktische Übungen und schließlich die Bewertung des Lernprozesses.

Online-Trainingsplattformen haben den Vorteil, dass sie den Mitarbeiter/Innen die Flexibilität bieten dann zu lernen, wenn es zeitlich bei ihnen geht. Jeder kann die Schulungen in seinem eigenen Tempo ausführen, wiederholen und sich selbst kontrollieren.

Administratoren haben beim Einsatz solcher Trainingsplattformen die Möglichkeit, über Security-Dashboards sowohl den Wissensstand als auch das Verhalten einzelner Mitarbeiter in der Praxis im Auge zu behalten und Nutzer gezielt anzusprechen, falls ihr Verhalten nicht adäquat erscheint.

Auch für das Personal des Rhein-Kreises Neuss ist ein regelmäßiges Angebot für ein IT Sicherheitstraining sinnvoll. Das Sensibilisieren mit aktuellen Informationen im Intranet sollte durch eine spezielle Schulungsform ergänzt werden. Hierzu arbeitet der IT-Sicherheitsbeauftragte an speziellen Schulungsangeboten für die Mitarbeiter/Innen der Kreisverwaltung.

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“.

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.

BSi 200-x
Durch die Umstrukturierung und Erweiterung des IT-Grundschutzhandbuchs im Jahr 2006 durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurden die Methodik und die IT-Grundschutz-Kataloge getrennt. Die BSI-Standards enthalten Angaben zum Aufbau eines Informationssicherheitsmanagementsystems (ISMS) (200-1), der Vorgehensweise nach IT-Grundschutz (200-2) und der Erstellung einer Risikoanalyse für hohen und sehr hohen Schutzbedarf (200-3).

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) (auch: „Allesnetz“;[1] englisch Internet of Things, Kurzform: IoT) 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.

ISO 27001
Diese internationale Norm spezifiziert die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Management-Systems unter Berücksichtigung des Kontextes einer Organisation.

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.

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.

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 2019/2020

Bildinhalte / Quellen

Piqsels.com - CCO Lizenz (S.1,9,12,14,18,20,22,24)
Bundesamt für Sicherheit in der Informationstechnik (S.3)
A. Woitschützke (S.2)
TÜV Rheinland (S.7)
Symantec (S.16,17)
Sketch Bubble (S.17)
Kaspersky (S.19,25)
Screenshots Applikationen Rhein-Kreis Neuss (S.15,17,21,23)

Impressum

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

Frank Meger
IT-Sicherheitsbeauftragter

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