rhein kreis neuss

Jahresbericht

IT-Sicherheit

Rückblick 2020

Ausblick 2021

Vorwort

Eine zunehmend digitale Welt bietet nicht nur Chancen, sondern birgt auch erhebliche Risiken. So ist nach dem jüngsten Digitalbarometer 2020 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bereits jeder Vierte in Deutschland Opfer von Cyber-Kriminalität geworden. Einer wachsenden Cyber-Kriminalität sehen sich auch Unternehmen, Institutionen und Behörden ausgesetzt.

Neben den steigenden, aber notwendigen finanziellen Investitionen in IT-Sicherheit kommt es vor allem auch auf den Menschen an. Es müssen zwar technische Vorkehrungen getroffen werden, sie allein können aber unsere Behörden-IT nicht vor allen Sicherheitslücken schützen. Um Malware und Phishing-Angriffe zu verhindern, sing gut geschulte Mitarbeiterinnen und Mitarbeiter wichtig. Entscheidend ist die präventive Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für die Informationssicherheit. Schulungs- und Sensibilisierungsmaßnahmen haben daher das Ziel, eine Sicherheitskultur und ein Sicherheitsbewusstsein (Awareness) in der Kreisverwaltung zu etablieren und auszubauen.

Das IT-Dezernat richtet sich bei der Informationssicherheit nach dem BSI-Standards. Hierzu baut der IT-Sicherheitsbeauftragte kontinuierlich ein Informationssicherheits-Managementsystem (ISMS) für die Kreisverwaltung auf. Der vorliegende IT-Sicherheitsbericht benennt die Schwerpunkte und Ziele unserer IT-Sicherheitsstrategie und gibt einen Überblick über die Vorhaben und Maßnahmen, die wir bereits gestartet haben und die wir für die Zukunft planen.

Die IT-Sicherheit bleibt im digitalen Wandel eine herausragende und permanente Herausforderung für Staat, Wirtschaft und Gesellschaft.

Harald Vieten
Dezernent für IT, E-Government und Bauen

Liebe Leserinnen und Leser,

im vorliegenden Bericht werden Sie viele Informationen zum Status Quo der IT-Sicherheit finden. Es liegt für Sie damit ein Rückblick auf die Aufgabenschwerpunkte aus dem Jahr 2020 vor, aber auch wieder ein Ausblick auf die notwendige Weiterentwicklung in der IT Sicherheit beim Rhein-Kreis Neuss.

Es wird auch die folgenden Jahre darum gehen, das erreichte Sicherheitsniveau ständig zu verbessern. Dazu müssen weitere Sicherheitsthemen umgesetzt beziehungsweise nach dem heutigen Wissensstand aktualisiert werden. Das bedeutet zusätzlichen finanziellen, personellen und zeitlichen Aufwand, um den zunehmenden Cyber-Bedrohungen effektiver gegenzuwirken.

Sie werden zu allen Artikeln drei verschiedene Piktogramme finden, die symbolisch für ein erforderliches Budget, einen zeitlichen und den personellen Aufwand stehen:

Finanzieller Aufwand zur Umsetzung und im laufenden Betrieb

Zeitlicher Aufwand zur Einführung und im laufenden Betrieb

Personeller Aufwand zur Einrichtung und im laufenden Betrieb

Anhand der Symbole soll Ihnen deutlich werden, welche dieser drei Ressourcen wie hoch belastet wird, um die beschriebene Aufgabe wahrzunehmen.

Es gibt viel zu tun, um in der Vorsorge gegen Cyber Kriminalität gut gerüstet zu sein. Lesen Sie bitte selbst.

Frank Meger
IT-Sicherheitsbeauftragter

Inhalt

Investieren in IT-Sicherheit

Ergebnisse des “Hiscox Cyber Business Report 2020”

Es gibt zahlreiche Studien zu den Entwicklungen in der Cyberkriminalität, die über den aktuellen Status und das Ausmaß der digitalen Angriffe berichten. Viele Studien belegen unter anderem, dass die finanziellen Schäden deutlich höher wie im Jahr 2019 ausfallen. Laut dem „Hiscox Cyber Business Report 2020“ war es im Jahr 2020 achtmal teurer als im Vorjahr, die Folgen eines Cyber Angriffs zu beseitigen.

Die Studie kommt auch zu der Erkenntnis, dass die Qualität der IT-Sicherheit beeinflusst werden kann. Das Sicherheitsniveau kann durch die richtigen Maßnahmen maßgeblich gesteigert werden. Die Studie fasst einige besonders wichtige Faktoren zusammen.

1. Finanzielle Ausstattung

In vielen Bereichen ist geplant, die Ausgaben für die IT-Sicherheit zu erhöhen. Man geht davon aus, dass sich im Angriffsfall wieder auszahlt, rechtzeitig für zusätzliche Schutzmaßnahmen investiert zu haben.

Ein Teil des IT Budgets sollte demzufolge fortlaufend in die Absicherung und Vorsorge von IT Risiken investiert werden. Nahezu alle Maßnahmen müssen dauerhaft betrieben werden.

2. Stabilisierte Infrastruktur

Eine gut ausgelegte Sicherheitsstrategie braucht ein stabiles Systemumfeld. Dazu zählen ein vollumfänglicher Endgeräte- und Serverschutz, ein aktuelles Patchmanagement, Firewalls, ein abgestuftes Rechtekonzept oder auch eine systembezogene Netzwerksegmentierung.

Genauso wichtig ist eine Sicherung der Unternehmensdaten außerhalb des produktiven Netzwerks. Alle Maßnahmen müssen durch regelmäßige Tests und simulierte Angriffe überprüft werden.

3. Prävention, Vorsorge und Vorsicht

Es kann nicht oft genug wiederholt werden: Um Malware und Phishing Angriffe zu verhindern sind vor allem gut geschulte Mitarbeiter gefragt. Es sind oft einfache, aber ständig geübte Verhaltensregeln, die sich enorm auf die IT Sicherheit auswirken.

Regelmäßige Schulungen und Sensibilierung betreffen die gesamte Belegschaft, auch die Führungsebene.

4. Gegen Restrisiken absichern

Auch unter der Beachtung aller Maßnahmen gibt es keine absolute Sicherheit. Deshalb gehört zu einem umfassenden Schutz auch eine Cyber-Versicherung. Sie sollte nicht nur eine finanzielle Deckung berücksichtigen. Für ein hohes Maß an Sicherheit muss externes Fachwissen für Präventionsmaßnahmen, Risikobewertungen, Krisenmanagement und Schulungen bereitstehen. Die Wahrscheinlichkeit, dass man Opfer einer Cyber Attacke wird, liegt laut vorliegendem Report fast zwanzig Mal höher als bei Diebstahl oder Feuer.

Live Ansicht laufender Cyberattacken innerhalb von 5 Sekunden

Quelle: Bitdefender

Cyberversicherungen – mehr wie ein finanzieller Schutz

Deutsche Unternehmen und öffentliche Einrichtungen liegen weiterhin besonders weit vorn im Fokus von Hackerangriffen. Positiv ist, dass die Anzahl der erfolgreichen Angriffe zurückgegangen ist. Umso alarmierender ist aber die Tatsache, dass die erfolgreichen Angriffe den Opfern zunehmend teurer zu stehen kommen.

Cyberresilienz aufbauen

Auch wenn es keinen vollständigen Schutz gibt kann die Widerstandsfähigkeit gegen Hackerangriffe durch Testläufe und regelmäßige Sicherheitsaudits verbessert werden. Eine zusätzliche Absicherung erreicht man durch eine spezialisierte Cyberversicherung, bei der es nicht nur um eine Kostenübernahme geht.

Es geht zusätzlich um die Identifikation von Sicherheitslücken, regelmäßige Personalschulungen als auch die Aufstellung und die Ausführung eines IT Krisenplans. Im Fall eines Angriffs müssen der Einsatz und die Kostenübernahmen für spezialisierte Dienstleister aus den Bereichen IT Forensik, Recht und Öffentlichkeitarbeit in einer Cyberversicherung inbegriffen sein.

Prävention, Soforthilfe & Schadensabdeckung

Bei der Wahl der Versicherung ist deshalb entscheidend, dass Assistance Leistungen, Soforthilfe und der Zugriff auf ein externes Expertennetzwerk in der Police inbegriffen sind. Ausschlüsse sollten nur im begrenzten Umfang die Dienstleistung beschränken und in dem Fall klar formuliert sein.

Die Verfügbarkeit beziehungsweise der Wiederanlauf einer gehackten IT Infrastruktur erfordert unter Umständen vielmehr Experten zur Schadensanalyse und Behebung, als dass finanzielle Untersützung hilft.

Wichtige Bausteine einer umfassenden Cyber Versicherung sind

- eine Cyber Eigenschadensdeckung.
- eine Cyber- und Werbe-Haftpflichtversicherung.
- die Deckung von Cyber-Betriebsunterbrechungen.
- Deckung des Verlusts durch Eigenschäden, zum Beispiel Fehlüberweisungen.

Wichtig ist die klare Definition von Cybervorfall-Auslösern und eine darauf abgestimmte präventive Vorsorge. Ein aktives Online Cybertraining kann Bestandteil einer solchen Versicherung sein und führt in der Regel zu einer reduzierten Selbstbeteiligung im Schadensfall.

Fazit

Eine parallele versicherungstechnische Absicherung gegen die erheblichen Risiken einer Cyberattacke hat aus allen vorgenannten Gründen ihre Berechtigung. Die Höhe der Beiträge muss beiderseitig ermittelt werden. Je nach bereits vorhandenem Sicherheitsniveau können Beiträge und die garantierten Schutzleistungen variieren.

E-Mails an den Rhein-Kreis Neuss
nur jede 10. E-Mail wird zugestellt

E-Mails an den Rhein-Kreis Neuss durchlaufen mehrere Prüfprozesse, bis sie das Postfach der Mitarbeiter erreichen. Federführend beteiligt bei der Analyse des Mailverkehrs ist das Rechenzentrum ITK Rheinland. Über 800.000 Mal im Monat wird versucht, dem Rhein-Kreis Neuss elektronische Post zuzustellen. Doch nur 9,5 Prozent dieser E-Mails werden tatsächlich als sicher eingestuft und übermittelt.

Jede dieser E-Mails muss verschiedene Prüfvorgänge bestehen, bevor sie zugestellt wird:

- Reputationsfilter
  Ankommende E-Mails werden nach deren Herkunft überprüft. In 90 % der Fälle kann man anhand der Herkunft auf Spam schließen. E-Mails mit negativer Herkunft werden abgelehnt.

- Spam-Quarantäne
  E-Mails werden im nächsten Schritt anhand verschiedener Kriterien (SenderBase) untersucht. Werden E-Mails als „Spam“ identifiziert oder wird ein „Virus“ erkannt, wird die betroffene E-Mail in eine Quarantäne verschoben. Bei falscher Interpretation (False Positive Mail) kann eine Zustellung nachträglich erfolgen.

- AntiVIR
  Zwei Virenscanner prüfen unabhängig voneinander die bis dahin angenommenen E-Mails auf Viren und verschieben identifizierte Viren-Mails in die Quarantäne.

- Virus-Outbreak
  Erkennt das System Merkmale, dass es sich ggf. um einen noch nicht entdeckten Virus handelt, wird die E-Mail automatisch zur Prüfung weitergeleitet. Virenscanner werden automatisch aktualisiert, um eine Verbreitung der Viren zu unterbinden.

Die gleiche Prozedur wird durch andere Schutzsoftware beim Rhein-Kreis Neuss wiederholt. Dieses mehrstufige Sicherheitskonzept hat sich bewährt und reduziert die Anzahl unseriöser E-Mails auf ein Minimum.

Sollte doch eine E-Mail mit verdächtigen Inhalten zugestellt werden kommen zwei weitere Prüfungen zum Einsatz. Sowohl die Anhänge in E-Mails und der Aufruf von verknüpften Webseiten werden erneut überprüft.

Last but not least:

Die Mitarbeiter müssen sorgfältig abwägen, ob eine E-Mail und deren Inhalt vertrauenswürdig ist. Eine hohe Aufmerksamkeit auf die restlich verbliebenen E-Mail Gefahren muss durch Schulungen und Sensiblisierung erreicht werden.

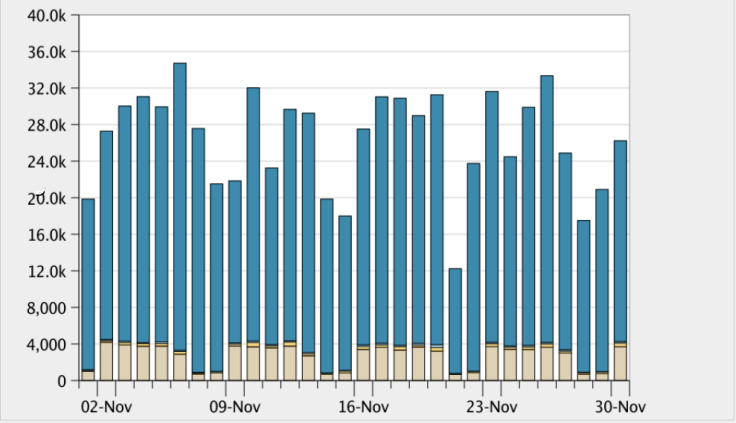
90 Prozent aller E-Mails werden herausgefiltert.

Als Beispiel die Auswertung des Monats 11/2020:
Von 800.000 E-Mails an den Rhein-Kreis Neuss werden nur noch 81.200 Nachrichten zugestellt

01 Nov 2020 00:00 bis 30 Nov 2020 23:59 (GMT +01:00)

Daten anzeigen für: Alle E-Mail-Appliances
Daten im Zeitbereich: 100.0 % abgeschlossen

Grafik der eingehenden Mails



Zusammenfassung der eingehenden Mails

Nachrichtenkategorie	%	Nachrichten
Gestoppt durch Reputationsfilterung	88.4%	707.4k
Gestoppt als ungültige Empfänger	0.5%	3,913
Spam festgestellt	0.9%	7,360
Virus festgestellt	0.0%	5
Gestoppt durch Inhaltsfilter	0.0%	125
Bedrohungen insgesamt:	**89.8%**	**718.8k**
Virenfreie Nachrichten	10.2%	81.2k
Gesamtanzahl der Nachrichtenversuche:		**800.0k**

Mitarbeiter für betrügerische E-Mails sensibilisieren

Nicht alle Phishing Mails werden automatisch erkannt. Das Erkennen von Gefahren in E-Mails, die trotz aller Filter zugestellt werden, obliegt damit den Empfängern.

Eine Phishing Simulation wird zu einem höheren Schutzniveau beitragen. Solche speziellen Trainings machen den Status der IT-Sicherheit messbar.

Sicherheitsexperten registrieren seit der Coronakrise eine starke Zunahme von Angriffsversuchen. Die Verunsicherung der Menschen wurde gerade zu Beginn der Pandemie durch E-Mails mit Schadsoftware begleitet. Das zunehmende Arbeiten im Home Office hat den elektronischen Nachrichtenverkehr zusätzlich verstärkt.

Warum sind Menschen für Phishing-Kampagnen empfänglich?

Die Angreifer nutzen das menschliche Verhalten aus. Hilfsbereitschaft, Neugierde oder Gier verleiten zum Öffnen von E-Mails und Anhängen, die mit einer Deadline einen Zeitdruck zum Reagieren aufbauen. Die Zahl der persönlich angepassten Phishing Mails hat dabei zugenommen.

Angreifer ermitteln im Vorfeld persönliche Informationen der Opfer über soziale Netzwerke oder die Firmenhomepage. So lassen sich Phishing Mails sozusagen „maßschneidern“.

Wie können IT Verantwortliche schützen?

Dazu gibt es keine Pauschalantwort oder eine einmalige Aktion, die hilft. Ein einfaches Schulungsvideo hat zum Beispiel keinen dauerhaften Effekt. Ziel muss es sein, dass Bewusstsein der Mitarbeiter kontinuierlich zu verbessern.

Dazu müssen dauerhafte Security Awareness Trainings, nicht nur zum Thema Phishing, durchgeführt werden. Es geht um unterschiedliche sicherheitsrelevante Themen, zu denen Beschäftigte sensibilisiert sein müssen.

Für den sicheren Umgang mit E-Mails sollten Phishing Simulationen durchgeführt werden. Somit lassen sich Erfahrungen mit bösartigen E-Mails sammeln, die in diesem Fall aber keinen Schaden anrichten. Für diesen Bereich wird der Wissenstand sogar messbar, nachdem die Ergebnisse der Kampagne ausgewertet sind. Der Handlungsbedarf für weiterführende Maßnahmen wird sichtbar.

Phishing Kampagnen laufen über mehrere Wochen und enthalten simulierte E-Mails in verschiedenen Sicherheitsstufen. Sie sind ein Schulungsbaustein, der bei der heutigen Bedeutung von E-Mails als wiederkehrendes Awareness Training etabliert sein sollte.

Neuer Schutzumfang für Server, PCs und Notebooks

Der Rhein-Kreis Neuss hat zum 3. Quartal 2020 seinen Programmeinsatz für den Schutz aller Rechnersysteme geändert. Alle Systeme wurden einheitlich mit einer Endpoint Protection Software mit zusätzlichen Schutzfunktionen ausgestattet. Wichtiges Ziel war die Erweiterung der Funktionen für alle schutzbedürftigen Systeme beim Rhein-Kreis Neuss.

Was bedeutet Endpoint Protection

Endpoint Protection ist die lokale Schutzkomponente aller Rechnersysteme zur Abwehr von Malware, Spyware und dient der Früherkennung weiterer schadhafter Angriffe auf die Betriebssysteme.

Die wahrscheinlich erste öffentlich dokumentierte Entfernung eines Computervirus mit einem Tool wurde von Bernd Fix im Jahr 1987 durchgeführt. Seitdem gibt es bei Antivirenprogrammen eine ständige Weiterentwicklung, um den neuen Angriffsmethoden mit unterschiedlichen Erkennungstechniken gegenzuwirken.

Inzwischen besteht ein wirksamer Schutz durch ein Zusammenspiel aus diversen Scanmethoden, heuritischer Erkennungsalgorythmen, Sandbox- oder Verhaltensanalysen, die durch Programmfunktionen der Endpoint Protection übernommen werden.

Für den vollständigen Schutz eines Rechnersystems sollte deshalb heutzutage ein **„Multi-Secured Endpoint“** Schutz eingeführt werden. Um das umzusetzen wurden beim Rhein-Kreis Neuss mit der Einführung der neuen Schutzsoftware zusätzliche Sicherheitsaspekte berücksichtigt.

Strategie: Der “MultiSecured” Endpoint

Durch eine einheitliche Verwaltung verschiedener IT Sicherheitsmaßnahmen mit einem Produkt können zusätzliche Programme eingespart, neue Funktionen hinzugewonnen und der Administrationsaufwand optimiert werden. Dazu wurden für den Rhein-Kreis Neuss die folgenden Leistungsmerkmale definiert:

- Einheitliche Endpoint Protection für alle Server, PCs und Notebooks.
- Vollständige Festplattenverschlüsselung für alle Notebooks, Desktop PCs und Server.
- Gerätekontrolle von USB Geräten und Speichermedien durch die gleiche Schutzsoftware.
- Automatisiertes Patch Management für Applikationen, die auf Servern installiert sind.
- Kontrolle erlaubter Applikationen durch gezielte Programmfreigaben.
- Einführung von „Endpoint Detection and Response“ (EDR).

Endpoint Detection and Response

Die Endpunkt-Gefahrenerkennung und die Einleitung von Reaktionen darauf ist eine komplexe Cyber-Sicherheitstechnologie. Für eine solche Verhaltensanalyse von Prozessen und Auswirkungen am Rechnersystem muss die Methodik “Endpoint Protection and Response” (EDR) zum Einsatz kommen.

Eine EDR Schutzkomponente bietet einzigartige Präventions-, Aufspürungs- und Abhilfemöglichkeiten. Diese Schutzfunktion reagiert sowohl auf bereits bekannte als auch auf unbekannte Varianten von Malware.

Im Gegensatz zu herkömmlichen Sicherheitsmethoden der Virenschutz-Programme und Firewalls bringt EDR eine größere Transparenz in das Verhalten am Endpunkt. Diese Schutztechnik ermöglicht dadurch schnellere Reaktionszeiten, wenn Bedrohungen auftreten.

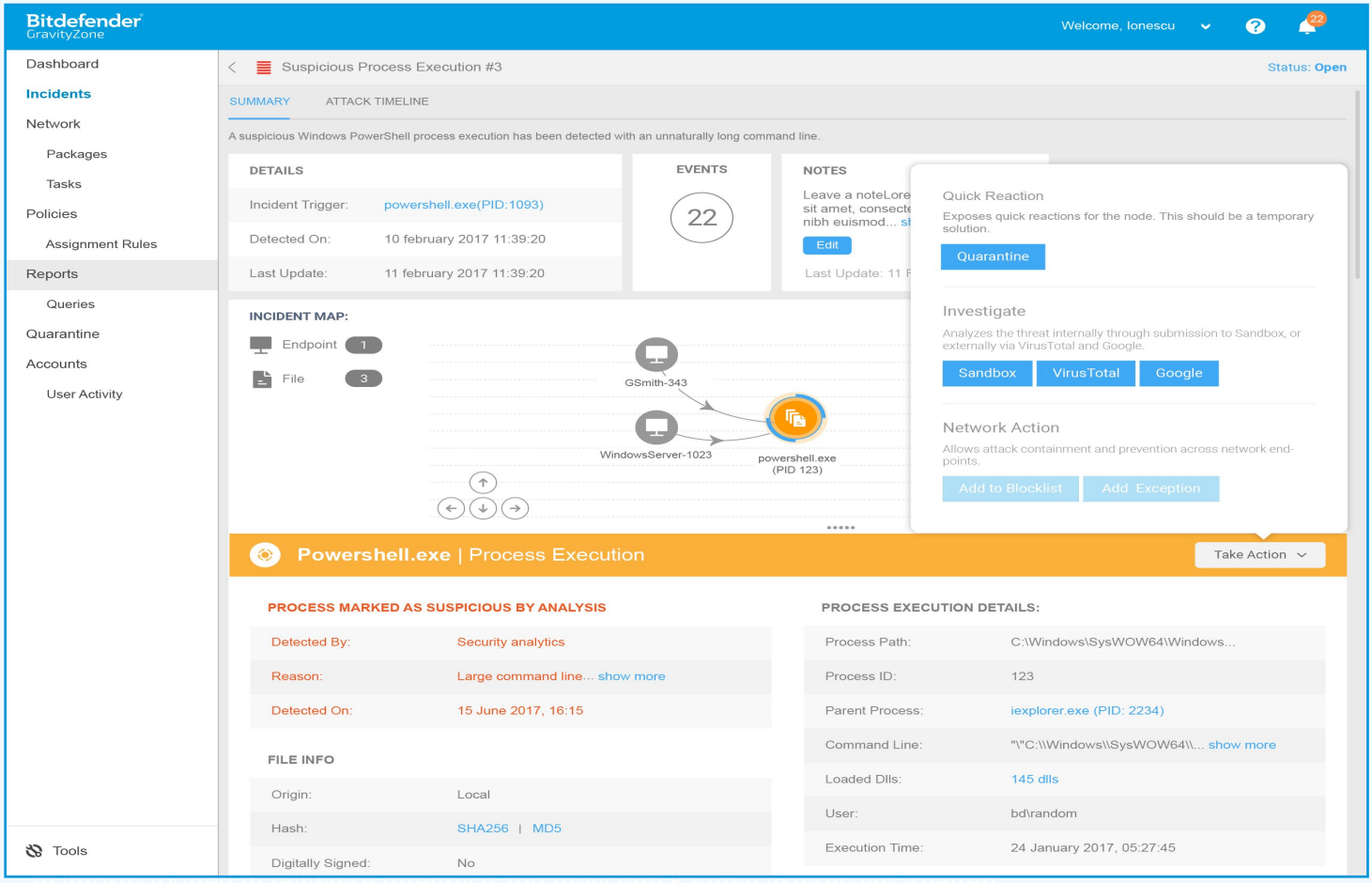
Die EDR-Fähigkeit als Teil einer vollständig integrierten Sicherheitsplattform schafft beim Rhein-Kreis Neuss eine einheitliche Lösung zur Endpoint Protection: Verhindern, Erkennen, Untersuchen, Reagieren und Weiterentwickeln mit einem Tool.

Erweiterte Schutzstrategie

Die Mehrwerte des neuen Softwareproduktes wurden als IT-Sicherheitsziel ab spätestens 2021 festgelegt. Mit der Einführung der neuen Endpoint Protection ist jetzt ein wichtiger Meilenstein für eine erhöhte Sicherheit der Rechnersysteme umgesetzt.

Der Einsatz von EDR Technologie bedeutet aber auch zusätzlichen Arbeitsaufwand bei der IT Systemadministration. Sobald eine Bedrohung identifiziert ist, führen Sicherheitsadministratoren Untersuchungen durch, lassen Dateien dezentral überprüfen oder senden Proben zur Verhaltensanalyse an den Hersteller der Schutzsoftware.

Die veränderten Methoden von Cyber Attacken erfordern kombinierte Produktlösungen, um eine bestmögliche Erkennung von Bedrohungen zu erreichen. Für den Rhein-Keis Neuss ist die “Multi Secured Endpoint” Strategie verpflichtend für alle Rechnersysteme umgesetzt.



Aufgabe für Systemadministratoren: Auswertung eines Sicherheitswarnung (Quelle: Bitdefender Insight Blog)

Rhein-Kreis Neuss setzt auf Spezialschutz für Daten

Schutzmaßnahmen gegen Ransomware

Die Daten des Rhein-Kreises Neuss befinden sich auf leistungsfähigen Speichersystemen des Anbieters Network Appliance. Nahezu 95 Prozent aller Daten sind auf diesen Speicherplattformen abgelegt. Deshalb gilt es hier ganz besonders, diese Daten vor Trojanern, Ransomware Attacken und anderen Hackerangriffen zu schützen. Eine immer häufiger werdende Methode der Angreifer ist es, die Daten in „Geiselhaft“ zu nehmen. Ein Zugriff auf die eigenen Daten wird nur nach der Zahlung eines Lösegelds wieder möglich sein.

Der Rhein-Kreis Neuss setzt bei den zentralen Speichersystemen deshalb einen speziellen Schutz gegen Ransomware Attacken direkt am Speichersystem ein. Dafür wird eine Schutzsoftware namens **“Cryptospike”** verwendet.

Quelle: Hackers Review

Wie funktioniert “Cryptospike”?

Cryptospike schützt die Speicherplattformen des Rhein-Kreises Neuss nach einem dreistufigen Konzept, das auf der Erkennung von Verhaltensmustern basiert.

Es werden Anomalien bei jeder Transaktion mit dem Dateisystem durch den Speichervorgang eines Anwenders erkannt. Bei der Interpretation eines ungewöhnlichen Zugriffs auf die Datenstruktur sperrt der Schutzalgorythmus den Lese- und Schreibzugriff des betreffenden Anwenders.

Zum Testen des Systems lassen sich harmlose, simulierte Malware Angriffe inszenieren. So lässt sich die Funktion des Schutzes prüfen und nachstellen.

Für die Erhöhung der IT Sicherheit ist die Installation von Cryptospike beim Rhein-Kreis Neuss eine wichtige Maßnahme. Sie ergänzt andere Schutzmaßnahmen wie Firewalls, Virenscanner etc. und setzt da an, wo inzwischen alle 40 Sekunden weltweiter Schaden verzeichnet wird: Das Verschlüsseln von Daten durch Ransomware.

Durch Ransomware infizierte Datenbestände betreffen oft die gesamte IT Infrastruktur. Durch diese spezielle Überwachung von Datentransaktionen ist der Datenbestand des Rhein-Kreises Neuss zusätzlich geschützt.

IT-Sicherheit auf die Probe gestellt - Penetrationstests

Knapp 70 Prozent der Unternehmen und Organisationen in Deutschland sind in den vergangenen Jahren Opfer von Cyber-Angriffen geworden. In knapp der Hälfte der Fälle waren die Angreifer erfolgreich und konnten sich zum Beispiel Zugang zur IT Infrastruktur verschaffen, die Funktionsweise von IT-Systemen beeinflussen oder diese nachhaltig stören. Jeder zweite erfolgreiche Angriff führte dabei zu schwerwiegenden, teils über mehrere Tage dauernden Produktions- bzw. Betriebsausfällen.

Was ist ein Penetrationstest?

Um die technische Sicherheitslage zu bewerten sollten regelmäßige Überprüfungen durchgeführt werden. Dazu bieten sich sogenannte „Schwachstellenscans“ an. Bei solchen Prüfungen werden die Systeme auf über mehrere Tausend Schwachstellen überprüft. Solche Prüfungen erfolgen meist automatisiert.

Bei einem Penetrationstest liegt die Aufgabe darin, Angriffe durchzuführen bzw. zu simulieren, wie sie auch durch Hacker ausgeübt würden. Mit dem Penetrationstest kann ermittelt werden, inwieweit ein möglicher Angriff auf die IT-Infrastruktur erfolgreich wäre und in welchem Ausmaß ein Schaden entstehen könnte.

Durch das Simulieren eines vorsätzlichen Angriffs auf die IT können die Wirksamkeit der vorhandenen Regelungen überprüft und fehlende Sicherheitsmaßnahmen erkannt werden.

Die Komplexität der heutigen IT Infrastruktur erfordert mehrere Penetrationstest pro Jahr. Der Fokus der Tests liegt auf verschiedene Bereiche:

- Externer Penetrationstest: Ziel ist die Überprüfung, ob von außen erreichbare Systeme wie Mailserver, Webserver etc. Schwachstellen aufweisen.
- Interner Penetrationstest: Bei einem internen Penetrationstest wird die Sicherheit aus Sicht eines Innentäters geprüft. Hierzu wird aus der Position eines normalen Mitarbeiters ein IT-Arbeitsplatz in der Verwaltung benutzt. Ziel ist es herauszufinden, zu welchen kritischen Daten und Systemen sich ein Angreifer aus dem internen Netzwerk Zugang verschaffen kann.
- Physischer Penetrationstest: Testen der physischen Sicherheit wie Zugangskontrollen, Berechtigungssysteme und die Awareness Ihrer Mitarbeiter. Wie weit kann ein Angreifer unbemerkt in die Firmenräumlichkeiten vordringen und Daten stehlen?

Alle vorangegangenen Techniken können über einen längeren Zeitraum als sogenannte **Red Team Simulation** (Long Term Assessment) angewendet werden.

Der Rhein-Kreis Neuss führt jährlich Penetrationstests durch. Der Umfang der personellen Begleitung und die notwendigen Vorarbeiten für einen Test muss in der IT Abteilung berücksichtigt werden.

Cyberattacken auf Behörden - Schwachstelle Mensch

Behörden, Krankenhäuser und andere öffentliche Einrichtungen werden immer wieder und zunehmend durch Cyberattacken lahmgelegt. Die Auswirkungen solcher Angriffe können das Einstellen kompletter Betriebsabläufe zur Folge haben. Die Veröffentlichung von Geschäftsgeheimnissen und persönlicher Daten kommt noch hinzu.

Die technischen Schwachstellen der IT sind nicht mehr das Hauptangriffsziel von Hackern. Die Angriffe richten sich vermehrt an die Mitarbeiter, denn mangelndes Sicherheitsbewusstsein und Unaufmerksamkeit im Online Datenverkehr stellen ein hohes Risiko dar. Sie werden immer mehr zu einem beliebten Angriffsziel.

Laut einer Studie mit dem Titel „People Centric Cybersecurity“ ist so gut wie jeder zweite IT-Sicherheitsbeauftragte in Deutschland der Meinung, dass ihre Mitarbeiter für Cyberangriffe anfällig sind. Erstaunlich ist dann aber, dass gut zwei Drittel der Verantwortlichen im Bereich der möglichen Schulungsmaßnahmen sparen. Das ist ein Widerspruch.

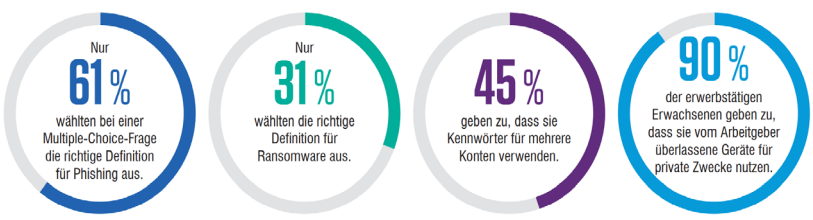
In der Praxis werden nach dem Ergebnis der Studie durchschnittlich maximal zweimal im Jahr entsprechende Schulungen durchgeführt. Dieser Wert gilt insbesondere für die Studienteilnehmer aus dem öffentlichen Sektor. Nicht einmal die Hälfte der Befragten konnte für seine Verwaltung behaupten, auf eine Cyberattacke vorbereitet zu sein.

Es besteht offensichtlich ein ständiger Handlungsbedarf zur dauerhaften und wiederkehrenden Sensibilisierung der Beschäftigten. Notwendige Schulungsprogramme und gezielte „Phishing Kampagnen“ trainieren die Beschäftigten für einen sicheren Umgang und das Erkennen von Cyber Attacken.

Zur Verbesserung der Awareness bei Mitarbeitern müssen folgende Ziele erreicht werden:

- Regelmäßige, wiederkehrende Security Awareness Kampagnen.
- Auswertung von simulierten Attacken.
- Planung von Folgemaßnahmen für einen höheren Lernerfolg.

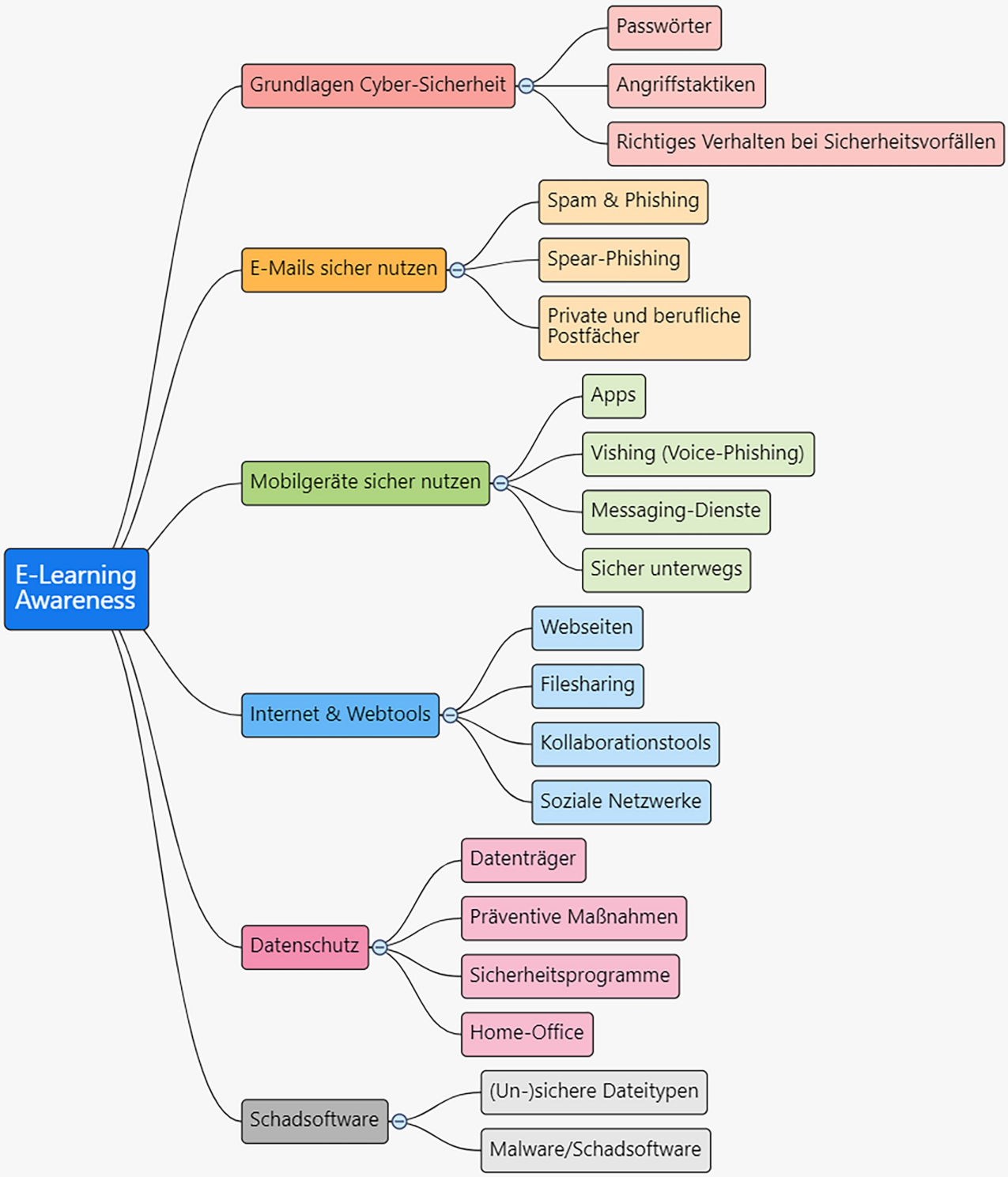
Lernprodukte und Awareness Kampagnen erfordern dauerhaft finanzielle Ressourcen. Für die Umsetzung und Begleitung muss zudem personeller Aufwand eingeplant werden.



Erkenntnisse aus dem „User Risk Report 2020“ der Fa. Proofpoint:
Wie gut sind Mitarbeiter zur IT-Sicherheit informiert?

Awareness Training: Verschiedene Lernmodule

Erkannte Lernziele für jeden Arbeitsplatz beim Rhein-Kreis Neuss



Phishing, Smishing, Vishing . . . Begriffe und ihre Bedeutung

Wer sich nicht umfassend mit den aktuellen Cyber Bedrohungen beschäftigt kann schnell verwirrt sein, was die Vielzahl der Fachbegriffe angeht. Inzwischen gibt es viele unterschiedliche Techniken, um Daten zu stehlen oder daran Schaden anzurichten. Hier einige Begriffe als Beispiel und die Antwort, wie gut wir uns auskennen.

Was ist Phishing?

Das klassische Phishing ist der älteste Begriff in diesem Artikel. Mit Phishing bezeichnet man die Aufforderung, als Reaktion auf betrügerische E-Mails persönliche, finanzielle oder sicherheitsbezogene Informationen preiszugeben. Diese E-Mails sind der Korrespondenz der Banken oder anderer Unternehmen im Text und Layout sehr ähnlich, denn Kriminelle hoffen, dass die Mailempfänger häufig E-Mails nur oberflächlich lesen.

Der Schaden entsteht durch das Öffnen eines Anhangs oder das Klicken auf einen Link, der zu einer unseriösen Webseite weiterleitet. Besonders bei mobilen Endgeräten, wie dem Mobiltelefon oder Tablet, kann es schwierig sein, den Phishing-Versuch zu erkennen.

Was ist Ransomware?

Mit Ransomware bezeichnet man Schadsoftware, mit der die Verwendung von Rechnern vollständig blockiert wird oder die Daten verschlüsselt werden. Für die Freigabe der Blockaden wird ein Lösegeld gefordert.

Bekannte Beispiele für diese Art von Malware sind Crypto Locker, WannaCry oder Locky.

Was ist Smishing?

Mit Smishing, bezeichnet man ein Phishing per SMS. Der Empfänger der Textnachricht wird dazu aufgefordert, einem Link zu folgen oder eine Telefonnummer anzurufen, um das eigene Konto zu „prüfen“, zu „aktualisieren“ oder zu „reaktivieren“. Das führt allerdings zu einer gefälschten Webseite oder im Fall einer Telefonnummer zu einem Kriminellen, der sich als Mitarbeiter des echten Unternehmens ausgibt.

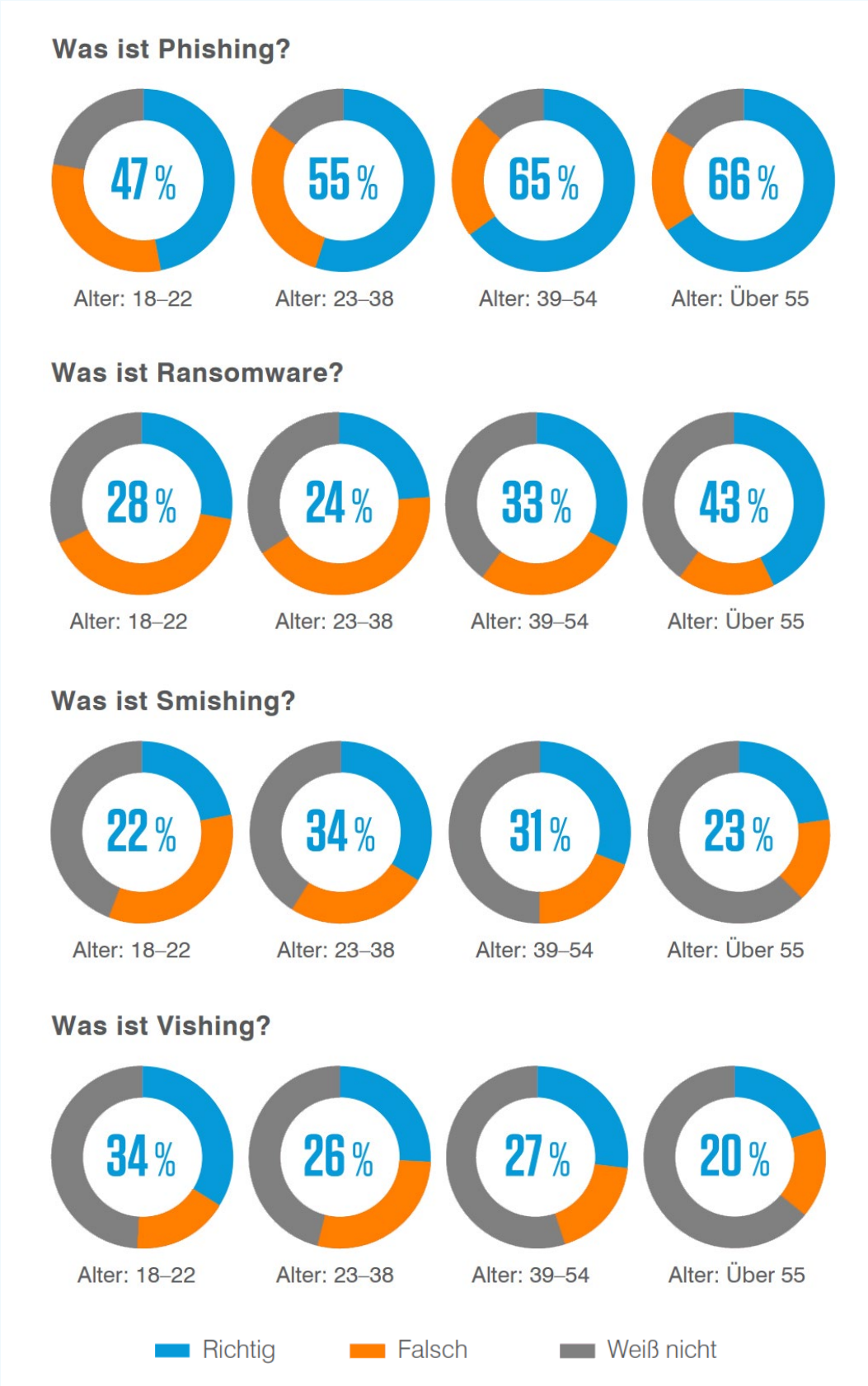
Was ist Vishing?

Der Begriff setzt sich aus den Worten „Voice“ und „Phishing“ zusammen. Bei dieser Methode soll das Opfer am Telefon dazu verleitet werden, seine Daten herauszugeben oder direkt Geld an die Kriminellen zu überweisen.

Zur Vorbereitung werden in den sozialen Medien persönliche Informationen des Opfers gesammelt. Es soll dazu verleiten dem Anrufer zu vertrauen, weil solche persönlichen Details bekannt sind. Im Zweifel sollte man sich die Telefonnummer geben lassen und einen Rückruf zusagen. So gewinnt man Zeit und kann die Telefonnummer der richtigen Organisation nachprüfen.

Aus der Studie User Risk Report 2020, Fa. Proofpoint:

Wie bekannt sind diese Begriffe in verschiedenen Altersgruppen?



Digitale Prozesse, Datenhaltung und deren Verfügbarkeit

Je stärker die Arbeitsabläufe von geschäftskritischen digitalen Anwendungen abhängen, desto größer sind die möglichen Folgen eines Ausfalls. Daher bilden Maßnahmen zur schnellen Wiederherstellung nach einem Ausfall (Disaster Recovery) einen wichtigen Teil einer ganzheitlichen Business-Continuity-Strategie.

Daten und ihre klassische Sicherung

Digitale Prozesse brauchen in der Regel eine serverbasierte Anwendung und speichern Informationen in Dateien und Datenbanken. Die gespeicherten Daten sind dabei eine unverzichtbare Grundlage. Es muss sichergestellt werden, dass diese Daten vor Verlust und Beschädigung geschützt sind. Ohne Serveranwendungen und der produzierten Daten läuft kein digitaler Prozess.

Aufgrund des ständig steigenden Datenwachstums ist die Fähigkeit, die Daten zu sichern, zu schützen und im Verlustfall wiederherzustellen, bei konventionellen Sicherungsmethoden eingeschränkt.

Das traditionelle Modell der vollständigen und inkrementellen Backups musste deshalb überdacht werden. Die Datengrößen wachsen und die Zeitfenster für vollständige Backups gehen eventuell über die SLA-Anforderungen hinaus. Insbesondere zu langwierige Wiederherstellungszeiten können ein weiteres Folgeproblem werden.

Neue Lösungsansätze

Eine zeitgemäße Data Protection & Recovery Lösung zeichnet sich dadurch aus, dass die Veränderungen und die aktiven Daten zusammen gespeichert werden. Beim Backup wird das bestehende Datenkonstrukt durch sogenannte **Snapshot-Technik** sozusagen eingefroren. Auf jeden gehaltenen Snapshot-Stand kann man sehr schnell zugreifen oder diesen wieder aktivieren.

Das Spiegeln der Daten auf ein zweites System und ein Tape-Backup sind zusätzlich genutzte Speicherziele.

Vorteile der Snapshot Technik

Es werden Verbesserungen bei den Sicherungszeiten erreicht, weil teilweise keine oder nur wenige Daten für die Snapshot-Erstellung bewegt werden. In noch größerem Maße werden aber Verbesserungen beim Wiederherstellen erzielt, da auch für große Restores teilweise keine Daten kopiert werden. Eine Datensicherung auf der Basis von Snapshots bedeutet also Zeitgewinn bei der Sicherung und dem Wiederherstellen von Daten.

Was tun beim Primärausfall

Die Sicherung wird direkt am produktiven Speicherpatz ausgelöst. Diese Primärdaten-Snapshots bieten zwar sehr effiziente Restore-Möglichkeiten, aber diese Technik benötigt einen zusätzlichen Schutz für den Ausfall dieses Primärdatensystems.

Es müssen zusätzliche Systeme mit gleichem Datenbestand in einem anderen Brandabschnitt verfügbar sein. Zusätzlich können Tape-Backups ergänzt werden, welche dann allerdings im Wiederherstellungsfall zeitverzögert eingesetzt werden.

Fazit

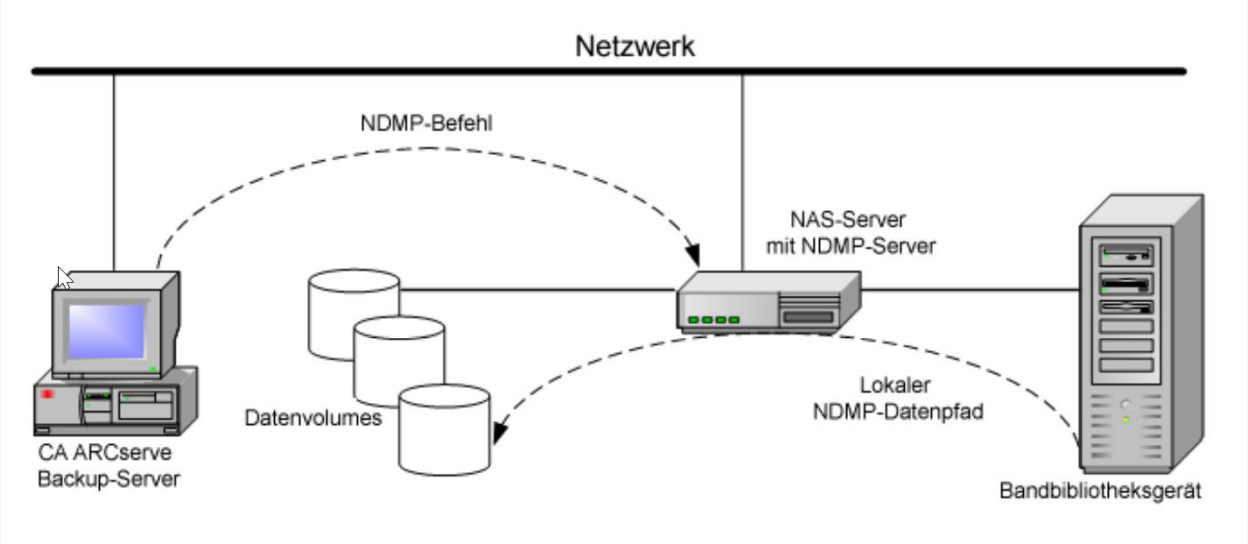
Für die Sicherung und die Wiederherstellung von Daten ist der Faktor Zeit entscheidend. Beim Rhein-Kreis Neuss sind Speichersysteme mit Snapshot Technologie und Bandsicherungen im Einsatz. 2021 werden zahlreiche Wiederherstellungstests durchgeführt, um die Performance zu bewerten und notfalls anzupassen.

Snapshot - wie es funktioniert

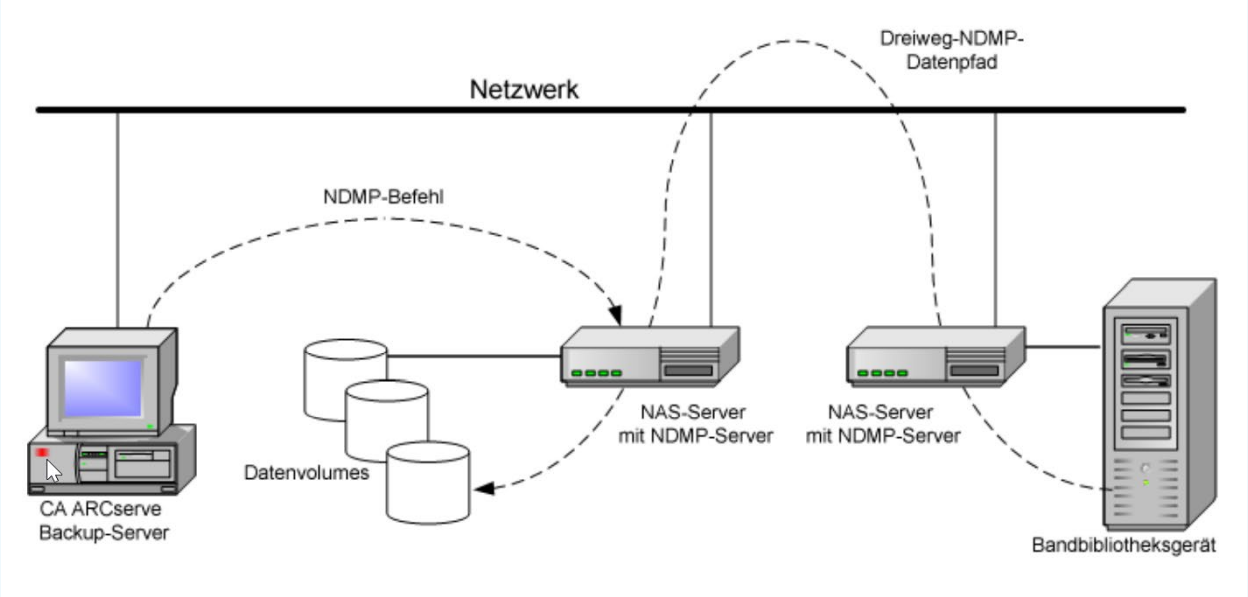
Snapshot Technologien sind eine wichtige Säule für heutige Backup- und Recovery-Konzepte. Ein wesentlicher Vorteil ist, dass beim Backup (der Snapshot-Erstellung) keine Daten kopiert werden müssen. Dies erlaubt extrem schnell abgeschlossene Primär-Backups und somit häufigere Sicherungen. Desweiteren wird das Erstellen konsistenter Backups erleichtert.

- Das Halten von einigen bis sehr vielen Snapshots über Tage bis Wochen ist möglich.
- Die Änderungszustände können in andere (sicher getrennte) Brandabschnitte kopiert werden.
- Die Verdichtung (Deduplizierung / Kompression) der Daten kann am Primär-Storage beginnen und bei der Replikation erhalten bleiben.
- Backups können auch vom Sekundär-Storage erfolgen, der Primär-Storage wird von der hohen Backup-IO-Last befreit.

Beispiel einer 3-Wege-Sicherung



Beispiel einer 3-Wege-Wiederherstellung



Security Information und Event Management (SIEM)

In einer komplexen IT-Infrastruktur gibt es zahlreiche Server, Netzwerkkomponenten und weitere Systeme, die bei der Datenverarbeitung beteiligt sind. Ein **Security Information and Event Management (SIEM)** ermöglicht einen ganzheitlichen Blick auf die IT-Sicherheit, indem Meldungen und Protokolle unterschiedlichster IT-Systeme gesammelt und ausgewertet werden. Verdächtige Ereignisse oder gefährliche Trends lassen sich dadurch in Echtzeit erkennen.

Für ein hohes Maß an Sicherheit ist die automatische Auswertung solcher Ereignisdaten wichtig. Durch das Sammeln und Auswerten von Meldungen verschiedener Geräte, Anwendungen und Security-Systeme in Echtzeit werden An-griffe und gefährliche Trends sichtbar.

Auf Basis der gewonnenen Erkenntnisse kann schnell und präzise auf Bedrohungen reagiert werden. Ein Security Information and Event Management nutzt für die Analyse ein Verfahren des maschinellen Lernens und der Künstlichen Intelligenz (KI).

Das SIEM bietet einen Überblick über sicherheitsrelevante Ereignisse in IT Umgebungen und hilft gesetzliche Vorgaben oder Richtlinien und Compliance-Regularien der IT-Sicherheit zu erfüllen. Sowohl die Echtzeit-Reaktion auf Bedrohungen als auch der nachträgliche Nachweis von Sicherheitsereignissen sind möglich.

Automatisierte Berichte und gezielte Alarmierungen erlauben dem IT-Sicherheitspersonal angemessen auf die unterschiedlichen Bedrohungen zu reagieren.

Auch beim Rhein-Kreis Neuss wächst die Zahl der eingesetzten IT Systeme und es besteht der Bedarf, von intern und extern auf Daten und IT Verfahren zuzugreifen. Das betrifft die Verwaltung, aber auch das heutige Arbeiten an Schulen und deren Anforderungen des virtuellen Lernens.

Deshalb wird es für die IT Verantwortlichen erforderlich, alle systemrelevanten Meldungen automatisiert zu sammeln und über ein Security Information und Event Management auszuwerten. Die Einführung und die Anbindung aller beteiligten IT Systeme wird für 2021 beziehungsweise abschließend bis 2022 vorgeschlagen.

Ziel ist der Aufbau einer effektiv automatisierten Lösung zur Benutzer- und Angreiferverhaltensanalyse, das Erfassen von Täuschungstechnologie (Angreiferfallen) sowie weitere innovative Elemente zur Erkennung von bekannten und unbekannten Bedrohungen.

Es soll die IT-Verantwortlichen durch eine umfassende Netzwerktransparenz für eine beschleunigte Bedrohungsanalyse vorbereiten.

Gartner definiert SIEM

„...als eine Technologie, die die Erkennung von Bedrohungen und die Reaktion auf Sicherheits-Incidents durch die Echtzeiterfassung, aber auch historische Analyse von Sicherheits-Events aus einer Vielzahl von Event- und kontextbezogenen Datenquellen unterstützt."

Eine analysegestützte SIEM-Lösung bietet sechs Kernfunktionen

ECHTZEIT-MONITORING	Da Bedrohungen laufend stattfinden und sich schnell verändern, braucht das IT-Team die Möglichkeit zur Überwachung und der Korrelation von sicherheitsrelevanten Events in Echtzeit. Damit können diese schnell entdeckt und gestoppt werden.
INCIDENT RESPONSE	Das IT-Team benötigt einen standadisierten Untermehmensprozess, um potenzielle Sicherheitsverletzungen sowie deren Folgen anzugehen und zu verwalten. Damit lässt sich der Schaden eindämmen und die Wiederherstellungszeit reduzieren.
BENUTZER-MONITORING	Das Monitoring von Benutzeraktivitäten mit Kontext ist äußerst wichtig, um Sicherheitsverstöße zu erkennen und Missbrauch aufzudecken. Das Monitoren priviligierter Benutzer ist eine häufige Anforderung für Compliance Berichte.
BEDROHUNGS-INFORMATIONEN	Bedrohungsinformationen können der IT-Abteilung helfen, das Risiko für die Verwaltung einzuschätzen und die Reaktion darauf zu priorisieren.
KOMPLEXE ANALYSEN	Analysen sind der Schlüssel zur Gewinnung von Erkenntnissen aus großen Datenmengen. Mit Machine Learning können diese Auswertungen automatisiert werden, um versteckte Bedrohungen aufzuspüren.
ERKENNUNG KOMPLEXER BEDROHUNGEN	Sicherheitsexperten benötigen spezielle Tools für das Monitoring, Analysieren und die Erkennung von Bedrohungen innerhalb der Bedrohungskette.

IT-Sicherheit im krisenbedingten Homeoffice

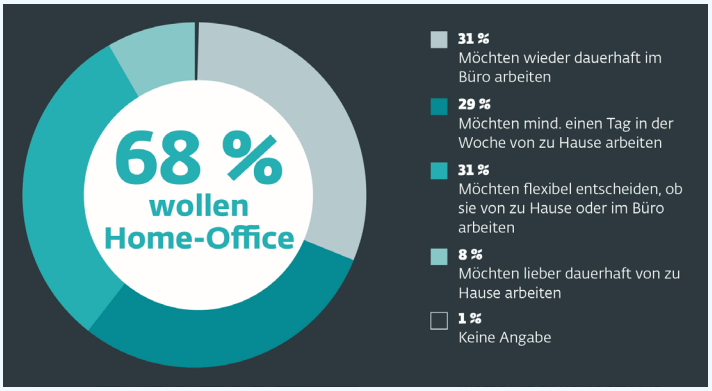
Durch die Corona-Krise ist die Zahl der Arbeitnehmer im Home Office deutlich angestiegen. Das Umstellen auf das mobile Arbeiten bedeutet zusätzliche Herausforderungen an die IT-Sicherheit. Der Rhein-Kreis Neuss hat dazu Vorkehrungen getroffen.

Im Homeoffice müssen in der eigenen Verantwortung die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität bei der Datenverarbeitung weiter beachtet werden. Es gibt sicherheitsrelevante Regeln nach dem IT Grundschutz, die zur IT-Sicherheit im Homeoffice beitragen.

Viele Beschäftigte kann man als ad hoc Homeoffice Anwender bezeichnen. Für dauerhafte Telearbeitsplätze gibt es klare Vorgaben, die für einen IT Grundschutz wichtig sind. Diese Anforderungen müssen auch bei zeitweiser mobiler Arbeit eingehalten werden.

Die Mitarbeiter werden zuhause ihr heimisches WLAN verwenden, um Datenverbindungen zum dienstlichen Netzwerk aufzubauen. Hierfür gelten die Vorgaben einer verschlüsselten Datenverbindung mit dafür freigegeben Rechnern des Arbeitgebers.

Was das Verarbeiten von Daten angeht: Das Sichern von lokalen Dateien wird am Heimrechner durch technische Richtlinien unterbunden.



Ein zusätzlicher Schutz der Festplatten wird durch die generelle Verschlüsselung der Datenträger erreicht. So wird auch im Falle eines Diebstahls ein lesbarer Zugriff auf die Daten des Rechners ausgeschlossen.

Die Schutzsoftware des Rechners hat im Homeoffice die gleichen Überwachungsfunktionen wie im Büro. Mit der VPN Verbindung zum Verwaltungsnetz des Rhein-Kreises Neuss erhält die zentrale IT Administration alle Warnmeldungen unabhängig vom Standort des Rechners.

Auch wenn in Krisenzeiten schnelle und pragmatische Lösungen gefragt sind, muss die IT-Sicherheit und Compliance berücksichtigt bleiben. Es muss sichergestellt werden, dass die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen im Home Office weiterhin gewährleistet sind und der Datenschutz berücksichtigt bleibt. Schwachstellen oder Kompromisslösungen müssen vermieden und allen Mitarbeitern bewusst sein. Sie haben zuhause eine besonders hohe Eigenverantwortung.

ESET Umfrage:
Wie Covid-19 unsere Arbeitswelt verändert

April 2020

Ihr Verhalten und Ihre Aufmerksamkeit sind wichtig.

- Sperren Sie den PC und schließen Sie die Tür ab, wenn Sie den Raum verlassen.
- Schließen Sie die Fenster, wenn niemand im Büro ist.
- Lassen Sie keine Ausdrucke im Drucker liegen.
- Legen Sie Unterlagen und sensible Daten in den verschlossenen Schrank.
- Lassen Sie Fremde und Besucher nicht alleine im Büro.
- Stellen Sie das Telefon bei Abwesenheit um.

Awareness Kampagne des Rhein-Kreises Neuss zur Sensibilisierung am eigenen Arbeitsplatz

IT-Sicherheit geht uns alle an.

„People Centric Cybersecurity“
Studie unter IT-Sicherheitsverantwortlichen

Das Kasseler Unternehmen techconsult, Anbieter von Informations- und Kommunikationstechnik, hat im Juli / August 2020 über 200 Unternehmen zu der Auswirkung von Cyberangriffen befragt und sich dabei auf vier Themenbereiche fokussiert:

- Wie häufig wurden Cyberangriffe durchgeführt?
- Wie war der Betrieb auf solche Angriffe vorbereitet?
- Welche Herausforderungen gibt es bei der Aufstellung von Cyberstrategien?
- Welche Auswirkungen hat die COVID-19 Pandemie auf die Cybersicherheit?

Das Ergebnis lässt sich auf alle Unternehmensbereiche, Organisationen und öffentliche Verwaltungen übertragen. Hier die wichtigsten Ergebnisse im Überblick.

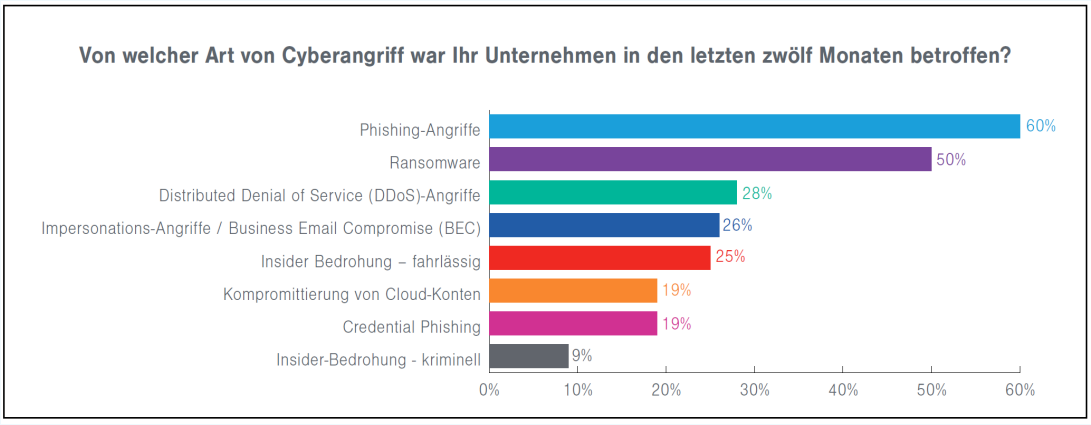
Verteilung der Bedrohungen

Zwei Drittel der Befragten konnten bestätigen, dass sie bereits einen Cyberangriff erlitten haben. Bei jedem Dritten konnten mehrfache Angriffe verzeichnet werden. Phishing und Ransomware haben immer noch einen hohen Bedrohungsgrad. Die Zahl der Insider Bedrohungen nimmt spürbar zu.

Laut Angabe der Studienteilnehmer kann jeder dritte Angriff auf Insider Bedrohungen zurückgeführt werden.

25 Prozent der Vorfälle sind Fahrlässigkeit und magelndem Wissen der Mitarbeiter zuzuschreiben.

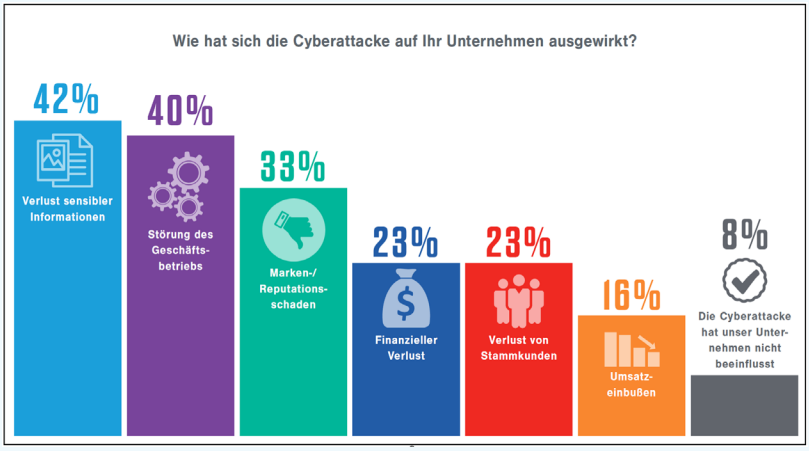
9 Prozent wurden druch einen böswilligen Datenmissbrauch verursacht.

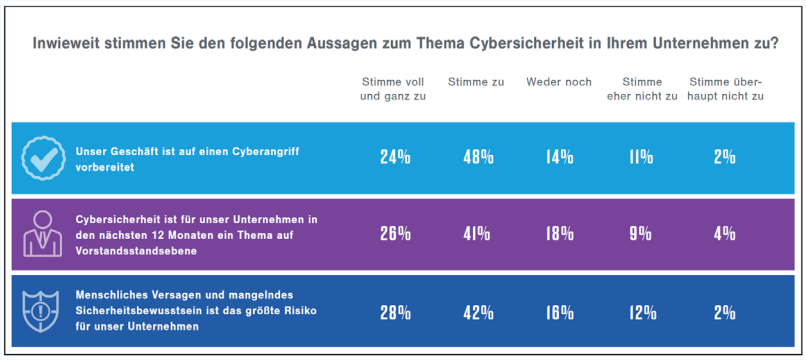


Auswirkung der Cyberangriffe

Die Auswirkungen von Cyberangriffen wurden von den Befragten zu mehreren Faktoren bewertet. Als häufigste Folge eines Cyberangiffs wird der Verlust von sensiblen Daten angegeben. Aber auch Störungen der Arbeitsabläufe, der Reputationsschaden und finanzielle Auswirkungen sind häufige Effekte eines erfolgreichen Cyberangriffs.

Lediglich 8 Prozent der Befragten gaben an, dass eine Cyberattacke keinen nennenswerten Einfluss gehabt hat.





Nur 24 Prozent der Befragten sind sicher, gut auf Cyberattacken vorbereitet zu sein.

Gefahr erkannt - Status der Vorsorge

Auch wenn sich die IT Verantwortlichen der Cyber-Risiken bewusst sind ist ein Ergebnis der Studie, dass die Vorbereitung auf Cyberangriffe für viele noch eine große Herausforderung darstellt. Nur jeder vierte Befragte fühlt sich auf digitale Attacken gut vorbereitet. In den öffentlichen Verwaltungen sind nur 46 Prozent davon überzeugt, umfassend gegen Cyberangriffe gerüstet zu sein.

Die Studie kommt zu dem Ergebnis, dass menschliche Fehler und ein geringes Sicherheitsbewusstsein als größte Risikofaktoren eingeschätzt werden.

Bewusstsein der Beschäftigten

Bei den Beschäftigten besteht offensichtlich ein hoher Bedarf zur Verbesserung von Sicherheitskenntnissen und -bewusstsein. Die üblichen Gefährdungen haben immer noch einen hohen Anteil als anfällige Risiken:

- 70% werden Opfer von Phishing Mails.
- 65% klicken auf schädliche Links.
- 52% verwenden unsichere Kennwörter.

Trotz der sich schnell entwickelnden Bedrohungslandschaft werden nur wenige Schulungen zur Cybersicherheit durchgeführt.

Da sich auch die Art und der Umfang der Bedrohungen verändern sollte ein regelmäßiges Schulungskonzept darauf abgestimmt werden.

Covid-19: Zunahme von Phishing

Mit Covid-19 hat weltweit der Anteil des mobilen Arbeitens in einem hohen Umfang zugenommen. Damit verbunden ist auch der Austausch von Informationen über E-Mail angestiegen.

Cyberkriminelle versuchen über gefälschte Websites Zugangsdaten zu erschleichen, wobei die Webseiten zunehmend in einem Zusammenhang mit staatlichen Hilfsleistungen oder anderen Themen mit Covid.19 Bezug stehen.

Wegen der Zunahme der persönlichen Cyberangriffe müssen gut informierte Beschäftigte zu einer verbesserten IT-Sicherheit beitragen.

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.

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.

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 2020/2021

Bildinhalte / Quellen

Arcserve (S.17)
Bitdefender (S.4)
ESET (S.20)
Pixabay.com - CCO Lizenz (S.5,6,8,10,11,12,14,16,18,20)
Proofpoint (S. 12,15)
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