Sachstandsbericht IT-Sicherheit beim VRR

Verkehrsverbund Rhein-Ruhr AöR
Verfasser: IT-Sicherheitsbeauftragter VRR AöR

IT-Sicherheit

Einleitung

Das Thema IT-Sicherheit gewinnt täglich an Bedeutung. Alle Aspekte des täglichen Lebens sind mittlerweile durch IT beeinflusst. Das wissen auch Kriminelle und versuchen kontinuierlich IT-Systeme anzugreifen, auch die IT-Systeme der VRR AöR. Daher ist es wichtig diese zu schützen, damit Vertraulichkeit, Integrität und Verfügbarkeit gewährleistet bleiben.

Die zentrale IT der VRR AöR möchte mit diesem Sachstandbericht darüber informieren, welche Maßnahmen der VRR bereits ergreift und welche für die Zukunft geplant sind, damit unsere Systeme bestmöglich geschützt werden. Aus Sicherheitsgründen werden keine tiefergehenden Details in diesem Bericht genannt.

Die Bereitstellung von IT-Systemen im VRR umfasst ein breites Spektrum unterschiedlicher Informationssysteme sowohl für den internen Gebrauch (Mailserver, Office, Arbeitsgeräte, Kopierer, u. ä.), als auch für die Kundensysteme (elektr. Fahrplanauskunft (EFA), PV-Ticketmanager, Ist-Daten-Server (IDS), Webseiten, gesicherte VPN-Verbindungen mit den VU u. v. m.). Insgesamt werden durch die zentrale IT des VRR über 250 virtuelle und physische Serversysteme in einer hochverfügbaren Infrastruktur betrieben. Diese unterschiedlichen Systeme benötigen spezielles Knowhow und Herangehensweisen, um sie bestmöglich abzusichern.

Zusätzlich ist der menschliche Faktor entscheidend für die IT-Sicherheit. Rein technische Lösungen wirken nicht, solange nicht jede*r Mitarbeiter*in im Unternehmen ebenfalls geschult und aufmerksam im Umgang mit den IT-Systemen ist. IBM[1] und andere[2] gehen davon aus das ca. 90 % der IT-Sicherheitsvorfälle auf menschliche Ursachen zurückzuführen sind (Hereinfallen auf Phishing Mails, unsichere Passwörter, fahrlässiger Umgang mit den Arbeitsgeräten).

[1] IBM Cyber Security Intelligence Index Report, June 2022
[2] After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk | World Economic Forum (weforum.org)

Zahlen, bitte…

Wie sehr IT-Systeme und Mitarbeiter*innen täglich angegriffen werden ist oft gar nicht sichtbar, denn glücklicherweise greifen viele Sicherheitsmechanismen bereits im Vorfeld. Damit das Ausmaß deutlicher wird folgend ein paar Zahlen aus dem Lagebricht 2022 des BSI.
Die Anzahl der Schadprogramme (Malware) ist im Berichtszeitraum um 116,6 Millionen Stück gestiegen. Im Jahr 2021 wurden 20.174 Softwareschwachstellen entdeckt, davon waren 13 % als kritisch eingestuft. In die deutschen Regierungsnetze wurden in diesem Jahr 34.000 Mails/Monat abgefangen (mehr als 1.000/Tag).

Die Firewall der VRR AöR hat, in der Zeit vom 1. bis 30. März 2023, 1.100 Bots und 2.200 Viren blockiert. Das Intrusion Protection System (Eindringschutz) hat in der Zeit 86.300 versuchte Einbrüche und die Firewall selbst hat 15,4 Mio. nicht erlaubte Zugriffe verhindert.

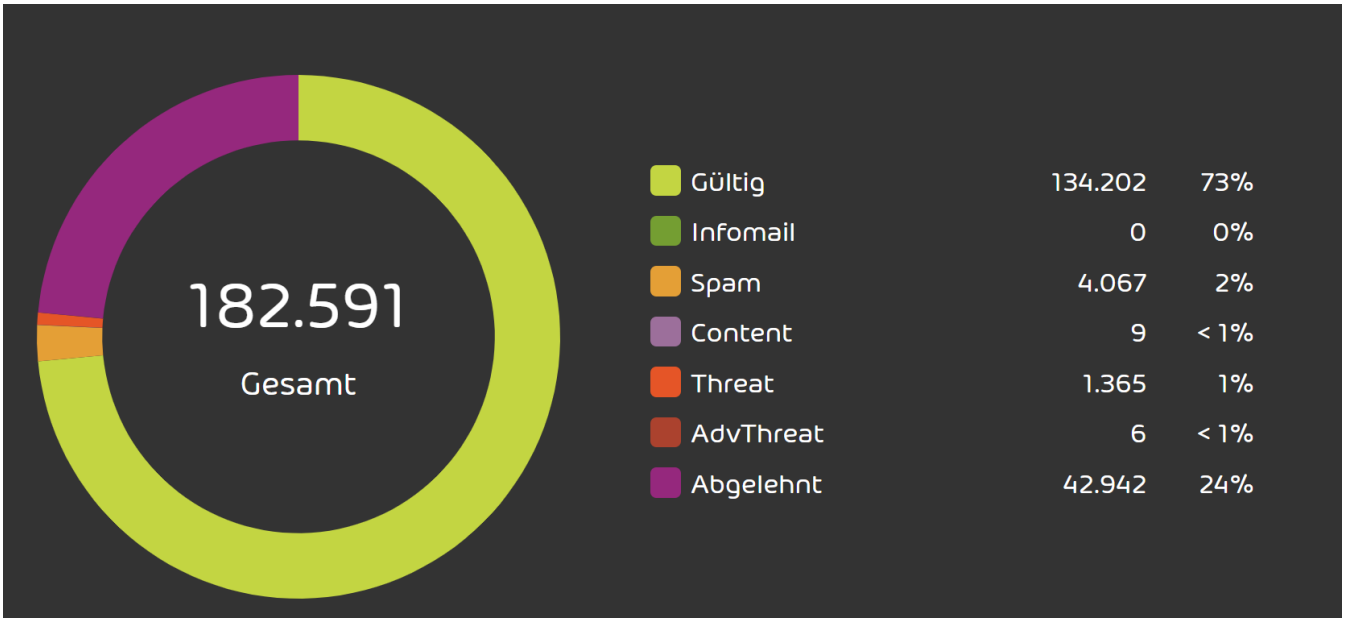

Abb. 1: E-Mail-Spamfilter im März '23

Der Spamfilter hat im März 2023 (Stand 30.03.) insgesamt 182.591 Mails gescannt, davon wurden 42.942 Mails abgelehnt (wegen bekannten SPAM-Adressen, ungültige Empfänger, leere Inhalte, ungültige Header, u. ä.), 1.371 Mails wurden als Schadsoftware erkannt und blockiert und 4.067 Spammails abgehalten. Das entspricht einem Viertel des gesamten Mailverkehrs eines Monats.

Schutzmaßnahmen im VRR

Netzwerksegmentierung

Um unberechtigte Zugriffe auf die unterschiedlichen Systeme zu minimieren, wird eine Netzwerksegmentierung eingesetzt, d. h. es gibt für die Anwendungsbereiche extra Netzwerke, welche untereinander ohne entsprechende Freigabe in der Firewall nicht miteinander kommunizieren können.
So gibt es ein Netz für Webserver, welche aus dem Internet erreichbar sein müssen, und weitere eigenständige Netze für intern genutzte Server oder VPN-Anbindungen. Arbeitsgeräte wie Notebooks befinden sich in einem eigenen Bereich, ebenso wie Smartphones und Tablets. Für Gäste gibt es ebenfalls ein eigenes Netz, so dass diese nicht auf interne Systeme zugreifen können. Abbildung 2 veranschaulicht das Prinzip.

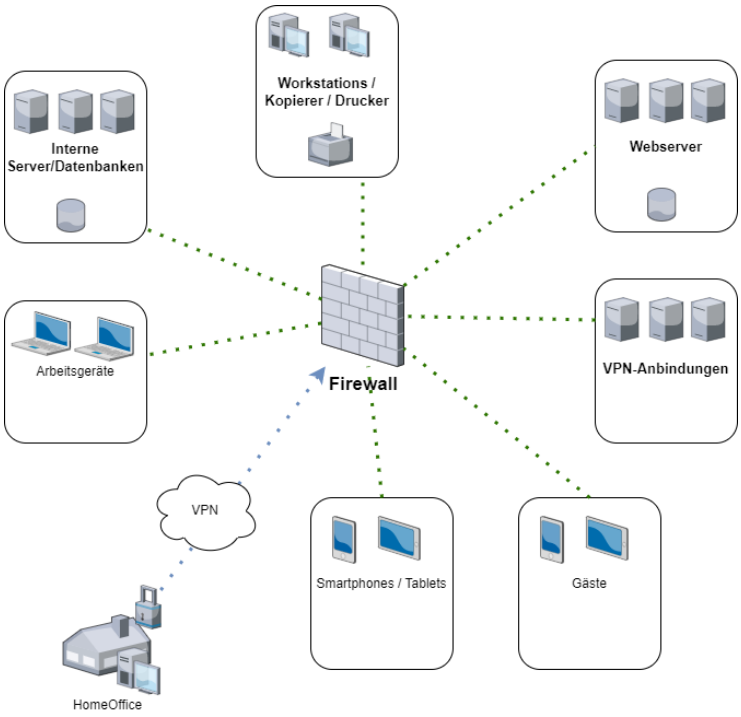

Abb. 2: Beispielhafte Netzwerksegmente im VRR

Firewall und Spamfilter

Wie bereits zuvor beschrieben, verwendet die VRR AöR zum Schutz ihrer Systeme eine Firewall. Diese ist redundant ausgelegt, so dass sollte es zu einem Ausfall eines Firewall-Gateways kommen, ein zweites Gateway direkt übernehmen kann. Die Firewall funktioniert als „Türsteher“ am Eingang der Netze der VRR AöR und lässt nur solche Datenpakete herein, welche explizit erlaubt wurden. Welche Pakete zu welchen Zielen dürfen, wird mit sog. Firewall-Regeln definiert. Damit soll gewährleistet werden, dass einzelne Systeme nicht zu viele Zugriffsrechte besitzen, welche im Fall einer Kompromittierung ausgenutzt werden könnten.
Im Bereich E-Mails setzt die VRR AöR einen Spamfilter-Dienstleister ein, welcher DSGVO konform arbeitet und seine Server im EU-Raum bereitstellt. Dieser Spamfilter überprüft

alle ein- und ausgehenden Mails auf Schadsoftware oder Spam und filtert diese ggf. heraus (s. o. Abb. 1).

Endpointschutz

Einzelne IT-Systeme werden durch Virenscanner und Anomalie-Erkennung geschützt. Sollte Schadsoftware erkannt werden, wird die IT darüber informiert und es können entsprechende Schritte eingeleitet werden. Zusätzlich werden die Mitarbeiter Endgeräte mit einem Mobile Device Management (MDM) verwaltet, welches es ermöglicht Geräte aus der Ferne zurückzusetzen, zu orten oder auch mit nötiger Software zu bestücken. Alle Festplatten der Geräte der VRR-Mitarbeiter*innen werden verschlüsselt, damit bei Verlust ein Auslesen der darauf gespeicherten Daten nicht möglich ist. Zusätzlich hat der/die Mitarbeiter*in auf seinem Arbeitsgerät keine administrativen Rechte und kann damit nicht selbstständig Software installieren. Die Mitarbeiter*innen sind durch das Datenschutz- und IT-Sicherheitshandbuch unter anderem dazu verpflichtet beim Verlassen ihres Arbeitsplatzes, den Computer zu sperren und ein ausreichend komplexes Passwort zu verwenden.

Penetrationstests

Die zentrale IT führt in regelmäßigen Abständen (aktuell alle 6 Monate) einen Penetrationstest für die aus dem Internet zu erreichenden Systeme der VRR AöR durch. Dabei scannt ein Dienstleister die extern erreichbaren Systeme und prüft diese auf Fehlkonfigurationen, nicht mehr aktuelle Software oder Sicherheitslücken. Diese werden durch den Dienstleister dokumentiert und der zentralen IT mitgeteilt. Die zentrale IT behebt dann die gefundenen Schwachstellen selbst oder in Zusammenarbeit mit weiteren Dienstleistern und Verantwortlichen. Der letzte Penetrationstest Ende 2022 hat folgendes ergeben:

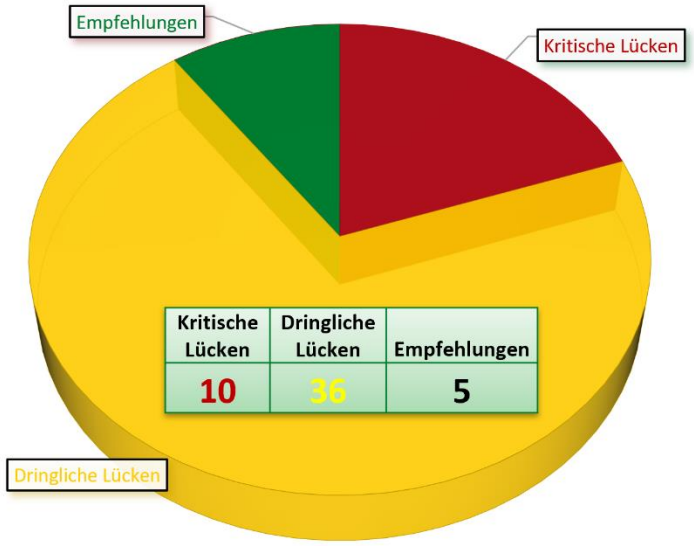

Abb. 3: Verteilung der gefundenen Schwachstellen

Es wurden 41 Schwachstellen gefunden, von denen 10 als kritisch eingestuft wurden. Diese kritischen Schwachstellen waren auf Softwareversionen von Webservern zurückzuführen, deren Support kurz zuvor ausgelaufen war. Diese wurden umgehend durch die zentrale IT behoben. Bei Systemen, welche durch einen Dienstleister gepflegt werden, wurde der Dienstleister informiert und angewiesen diese Schwachstellen zu beheben. 36 weitere gefundene Schwachstellen wurden als dringlich eingestuft und innerhalb von 4 Wochen nach bekannt werden behoben. Diese ergaben sich aus älteren Versionen von Frameworks oder nicht mehr aktuellen Einstellungen von Systemen. Die Empfehlungen wurden aufgenommen und wo möglich umgesetzt. Hierbei handelt es sich um Vorschläge zum Einsatz von Verschlüsselungsalgorithmen, welche nicht bei allen Systemen, aufgrund von Kompatibilitäten, umgesetzt werden konnten. Diese Empfehlungen stellen aber vorerst kein Sicherheitsrisiko dar. Der nächste Penetrationstest ist für Mitte des Jahres 2023 angesetzt.

IT-Awareness Training

Wie zu Beginn erwähnt ist der Faktor Mensch das größte Risiko in der IT. Daher ist es unerlässlich die Mitarbeiter*innen zu sensibilisieren und zu schulen. Die VRR AöR hat daher in Zusammenarbeit mit einem Dienstleister (SoSafe GmbH) ein IT-Awareness Schulungsportal aufgebaut, in dem die Mitarbeiter*innen wichtige Themen der IT-Sicherheit in kompakten Modulen und Abschlussfragen lernen und festigen. Über diese Plattform wird auch eine Phishing-Simulation durchgeführt. Dabei bekommen die Mitarbeiter*innen in zufälligem Abstand Phishing-Mails geschickt. Sollte ein*e Mitarbeiter*in eine dieser Mails öffnen, gelangt der/die Mitarbeiter*in auf eine Hinweis-Seite, die darüber aufklärt, wie gefährlich dieses Verhalten sein kann und dass im eLearning-Portal nochmal die passenden Module angeschaut werden müssen. Die erste Simulation zeigte, dass 9,4 % der Mitarbeiter*innen auf eine Phishing-Mail nicht korrekt

reagiert haben. Daher fokussiert die erste Schulungsphase der Mitarbeiter*innen auch auf die Erkennung von Phishing.

Aktuelle Angriffe: DDoS

Im März war die VRR AöR zweimal von einen sogenannten Distributed Denial of Service (DDoS) Angriff betroffen. Bei einem DDoS Angriff werden die Systeme des Opfers mit Millionen von Anfragen in kurzer Zeit überlastet mit dem Ziel die Systeme zum Absturz zu bringen oder mindestens ihre Erreichbarkeit einzuschränken. Den ersten DDoS Angriff erlitt die VRR AöR am 13.03.2023 in zwei Phasen. Einmal von 00:51 Uhr bis 03:54 Uhr und von 04:42 Uhr bis 05:16 Uhr. In dieser Zeit waren die Systeme des VRR nicht mehr erreichbar. Ungeklärt ist dabei das genaue Ziel des Angriffs und die Absicht. Die Uhrzeit lässt vermuten, dass die Störung des Betriebes nicht das Ziel gewesen ist. Es wird vermutet, dass es ggf. ein Testlauf gewesen sein könnte. Einen weiteren Angriff gab es am 27.03.2023, von 16:48 Uhr bis 17:04 Uhr. Wieder war die Erreichbarkeit der VRR-Systeme eingeschränkt. Die sehr kurze Dauer des Angriffs lässt die Absicht dahinter unklar. Zudem konnten als Ziele diesmal 2 Domains durch die Gelsen-Net (Provider) ausgemacht werden.
Die zentrale IT hat bereits nach dem ersten Angriff den Ausbau unserer Schutzmaßnahmen geprüft. Das Problem bei DDoS Angriffen liegt darin, dass der verursachte Traffic die Internetleitung zum VRR auslastet und blockiert, so dass on-premise Schutzmaßnahmen (selbstgehostet am eigenen Standort), wie sie der Loadbalancer und die Firewall mitbringen, keine Wirkung zeigen. Es müssen bereits Maßnahmen ergriffen werden, bevor der Traffic beim VRR ankommt. Dazu befindet sich die zentrale IT in Gesprächen mit der Gelsen-Net, welche erweiterte Schutzmaßnahmen man anbieten kann mit einem Partner, welcher den Internet-Traffic direkt am zentralen Knotenpunkt der DECIX in Frankfurt prüfen und filtern kann. Diese Maßnahme wird kurzfristig zusätzlich ergriffen.

Weitere IT-Sicherheitsmaßnahmen

Zusätzlich werden administrativen Zugänge mit einer 2-Faktor Authentifizierung abgesichert, wobei zusätzlich zum herkömmlichen Passwort noch ein weiterer einmalig gültiger Code benötigt wird (ähnlich einer TAN beim Banking). Die zentrale IT ist aktuell auch in der Ausschreibung für einen Dienstleister, um ein ISMS (InformationsSicherheitsManagementSystem) aufzubauen und eine ISO 27.001 Zertifizierung zu erhalten.