Sachstandbericht IT-Sicherheit beim VRR

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

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 aktualisierten 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, uvm.). Insgesamt werden durch die zentrale IT des VRR über 250 virtuelle und physische Serversysteme in einer hochverfügbaren Infrastruktur betrieben. Diese unterschiedlichen Systeme benötigen spezielles Know-How 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 und andere 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).

Zahlen, bitte…

Mails

Der Spamfilter In den letzten 3 Monaten (Stand 23.07.-23.10.2023) insgesamt 574.651 Mails gescannt, davon wurden 185.662 Mails abgelehnt (wegen bekannten SPAM Adressen, ungültige Empfänger, leere Inhalte, ungültige Header, u.ä.), davon waren 3.442 Mails als Schadsoftware und 11.117 als Spam klassifiziert. Das entspricht circa einem Drittel des gesamten Mailverkehrs der letzten drei Monate.

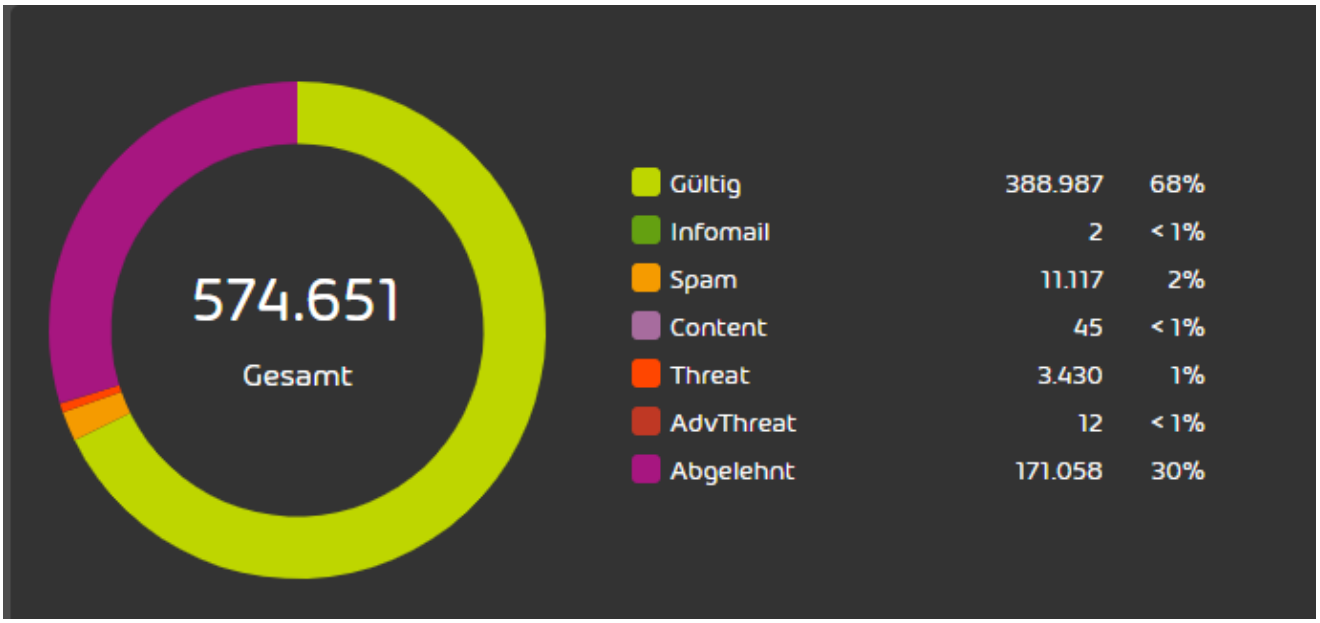

Abb. 1: E-Mail Spamfilter der letzten 3 Monate (23.07.-23.10.2023)

DDoS-Attacke

Seit dem letzten Sachstandbericht IT-Sicherheit wurde die VRR AöR, wie auch weitere deutsche Verkehrsverbünde Ziel eines koordinierten DDoS-Angriffs. Hierbei hatte eine Hackergruppe die Webseiten diverser Verkehrsverbünde in Deutschland angegriffen. Die Angriffe begannen am Freitag den 08.09. und gingen bis Montag, den 11.09.2023. Der Angriff hat zu Ausfällen der VRR Webseite und der Auskunft geführt. Die VRR-IT hat in Zusammenarbeit mit der Gelsen-Net als Internet-Provider und eines Dienstleisters im Bereich der Firewall/Schutzsysteme die Erreichbarkeit wieder herstellen können und kurzfristig weitere Schutzmaßnahmen gegen weitere Angriffe umgesetzt. Im Nachgang zu diesen Angriffen erfolgten noch weitere Angriffe auf andere Unternehmen aus dem Bereich des öffentlichen Personenverkehrs, der VRR war von diesen allerdings nicht betroffen.

Der Angriff wurde sowohl dem BSI - Bundesamt für Sicherheit in der Informationstechnik gemeldet als auch zur Anzeige gebracht.
Basierend auf den gewonnenen Erkenntnissen erfolgten weitere Maßnahmen, die unter DDoS Schutzmaßnahmen skizziert werden.

Schutzmaßnahmen im VRR

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 Mitte 2023 hat folgendes ergeben:

Es wurden 11 Schwachstellen gefunden, von denen 3 als kritisch eingestuft wurden. Dies stellt eine große Verbesserung zum Ergebnis des letzten Penetrationstests von Ende 2022 dar. Die gefundenen kritischen Schwachstellen waren auf Softwareversionen von Verschlüsselungssoftware (OpenSSL) zurückzuführen. Diese wurden umgehend durch die zentrale IT behoben. 8 weitere gefundene Schwachstellen wurden als dringlich eingestuft und innerhalb von 4 Wochen nach bekannt werden behoben.

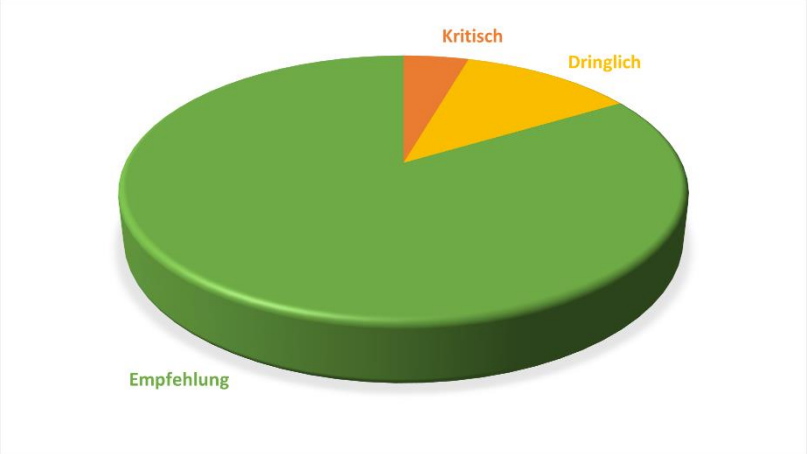

Abb. 2: Verteilung der gefundenen Schwachstellen

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 Ende 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 auf 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. Seit Anfang des Jahres 2023 steht beim VRR die Schulungsplattform zur Verfügung und bereits 94% der Mitarbeitenden sind im Tool aktiv (Zu den fehlenden 6% zählen neu hinzugekommene, langzeiterkrankte und sich bspw. in Elternzeit befindende Mitarbeitende).

DDoS-Schutzmaßnahmen

Zum Schutz der Kundensysteme hat die zentrale IT bei der Gelsen-Net einen erweiterten Schutz für die externen IP-Adressen der wichtigsten VRR-Dienste beauftragt (Layer 4 Schutz). Im Rahmen des großen DDoS Angriffs im September (s.o.) wurde dieser Auftrag nochmal um weitere Adressen erweitert. Mit einem Dienstleister wurde zu diesem Zeitpunkt ebenfalls ein weiterer DDoS-Schutz (Web Application Firewall / Layer 7 Schutz) kurzfristig aufgebaut. Dieser wird aktuell in einem Proof-Of-Concept weiter getestet und in den nächsten Wochen fest beauftragt. Auch in Bezug auf die Zusammenarbeit mit dem Internet-Provider sind weitere Maßnahmen geplant, um sowohl die Information und Kommunikation als auch die Ausfallsicherheit zu verbessern.

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, in Zusammenarbeit mit einem Dienstleister, in der Vorbereitung ein ISMS (InformationsSicherheitsManagementSystem) aufzubauen und damit auch eine ISO 27.001 Zertifizierung für die identifizierten Bereiche zu erhalten.