Sachstandsbericht 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 Sachstandsbericht 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, dass 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 hat in den letzten 3 Monaten (Stand 15.01.-15.04.2024) insgesamt 334.030 eingehende Mails gescannt, davon wurden 32.507 Mails abgelehnt (wegen bekannten SPAM-Adressen, ungültige Empfänger, leere Inhalte, ungültige Header, u.ä.), 5.683 Mails waren als Schadsoftware und 27.186 als Spam klassifiziert. Das entspricht circa einem Fünftel des gesamten eingehenden Mailverkehrs der letzten drei Monate. Anteilig ist die Anzahl der als Malware geblockten Mails deutlich gestiegen im Vergleich zum letzten Sachstandsbericht.

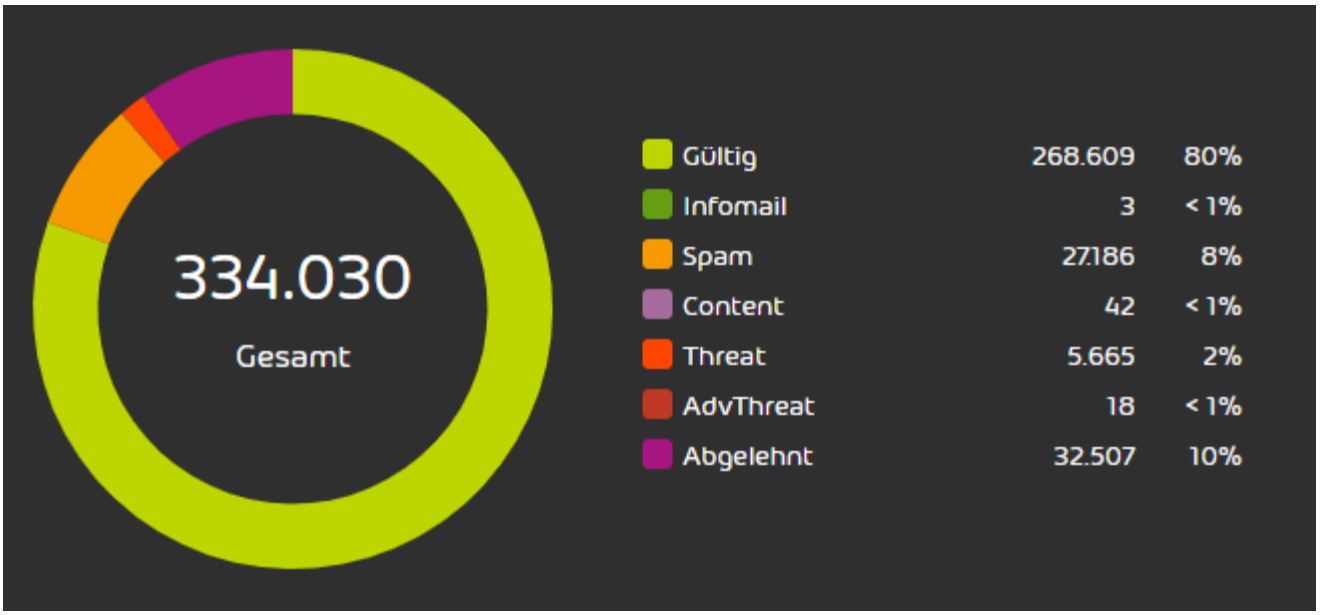

Abb. 1: E-Mail Spamfilter der letzten 3 Monate (15.01.-15.04.2024)

DDoS-Attacken

Seit dem letzten Sachstandsbericht IT-Sicherheit wurde die VRR AöR nicht wieder Ziel eines großangelegten DDoS-Angriffs. Die eingesetzten und erweiterten Schutzmechanismen haben kleinere Auffälligkeiten in den Verbindungen an die Systeme des VRR erfolgreich herausgefiltert und abgewehrt. Weiterhin besteht jedoch eine hohe Gefahr Ziel von erneuten Angriffen zu werden und der weitere Ausbau der Schutzmaßnahmen sowie kontinuierlicher Prüfungen dieser Schutzmaßnahmen ist zwingend erforderlich.

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 Anfang 2024 hat folgendes ergeben:

Es wurden 123 Schwachstellen gefunden, von denen 1 als kritisch eingestuft wurde. Die gefundene kritische Schwachstelle war auf eine unsichere Softwareversion (PHP) zurückzuführen. Diese wurde umgehend durch die zentrale IT behoben. 40 weitere gefundene Schwachstellen wurden als dringlich eingestuft und zeitnah nach Freigabe des Softwareherstellers behoben.

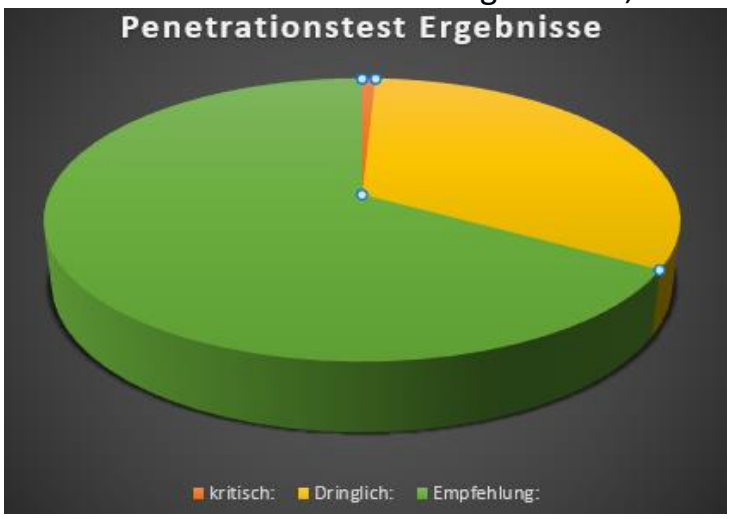

Abb. 2: Verteilung der gefundenen Schwachstellen

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. Im Ergebnis gab es dieses Mal weniger kritische Funde als beim letzten Test vor einem halben Jahr. Der nächste Penetrationstest ist für Mitte des Jahres 2024 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 Hinweisseite, die darüber aufklärt, wie gefährlich dieses Verhalten sein kann und dass im eLearning-Portal noch einmal die passenden Module angeschaut werden müssen. Seit Anfang des Jahres 2023 steht beim VRR die Schulungsplattform zur Verfügung und bereits 99% der Mitarbeitenden sind im Tool aktiv und 87% haben alle Lektionen bereits erfolgreich absolviert (Zu den fehlenden Prozenten zählen neu hinzugekommene, langzeiterkrankte und sich bspw. in Elternzeit befindende Mitarbeitende). Die jüngste Vergangenheit hat gezeigt, dass diese Angriffsszenarien sehr real sind und die Aufmerksamkeit der Mitarbeiter*innen eine wichtige Rolle spielt, da die VRR AöR seit dem letzten Sachstandsbericht von übernommenen Mail Accounts von Kommunikationspartnern mit entsprechenden Mails konfrontiert wurde. Dank der geschulten Mitarbeiter*innen konnte Schaden auf Seiten der VRR AöR abgewendet werden.

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 3 Schutz: Schutz vor Angriffen auf IP-Ebene, bei welchem Eigenschaften des TCP-IP Protokolls ausgenutzt werden.). Zusätzlich befindet sich ein Layer-7 DDoS Schutz (Web Application Firewall: Hier werden Angriffe auf Applikationsebene abgewehrt.) im Einsatz, welcher noch weiter durch die zentrale IT im Laufe dieses Jahres ausgebaut wird.

Weitere IT-Sicherheitsmaßnahmen

Zusätzlich werden administrative 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 27001 Zertifizierung für definierte Teilbereiche des VRR zu erhalten.
Zudem wurde ein neues Firewall-Konzept erstellt, welches im Laufe des Jahres umgesetzt wird, ebenso wie eine Multiprovider Anbindung, um die Ausfallsicherheit der Auskunftssysteme und weiteren Kunden- und Managementsysteme weiter zu erhöhen.