Outbound SPAM Protection mit selbst lernendem Authentifizierungsbackend

TÜV NORD CERT
DIN EN ISO 9001:2015

Das

anna69

Problem

- Ahnungslosigkeit,
- Gleichgültigkeit,
- Bequemlichkeit.

Alle Argumentationen zum Gebrauch sicherer Passwörter sind erfolglos!

Das

Ergeb-nis

solchen Verhaltens..

Welches

Ziel

wollen wir erreichen?

- Wir dürfen, auch über kompromittierte Accounts, keinen SPAM ausliefern.
- Wir wollen keine Accounts sperren und keine Passwörter ändern.
- Unsere Mailserver sollen für SPAMMER nachhaltig unattraktiv werden.
- Wir müssen den Aufwand für die Administration drastisch reduzieren!

Analyse (I)
Wie funktionieren

SPAMMER

eigentlich?

Spammer sind Kriminelle!

- Geschwindigkeit ist alles..
- Eine große Anzahl von Ressourcen wird gleichzeitig eingesetzt.

Dieses Verhalten ist der

Schlüssel zu einer

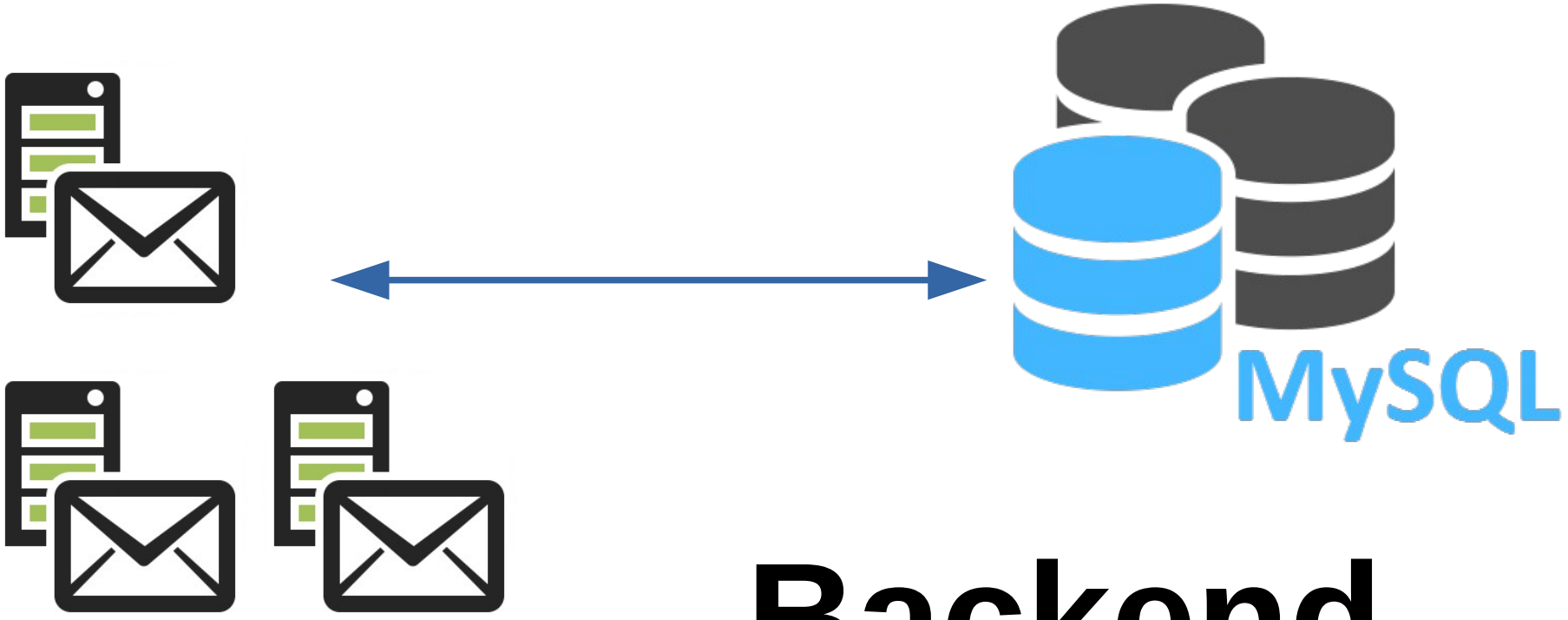
erfolgreichen Abwehr von SPAM!

Analyse (II)
Welche

Mittel

stehen uns zur Verfügung?

- Wir wollen aus Gründen der Komplexität so wenig wie möglich an den Konfigurationen unserer MTA's experimentieren.
- Aus dem Bereich der Softwareentwicklung gibt es bei uns Skills im Bereich Datenbanken.
- Die Authentifizierung für unsere Mail Server läuft über ein MySQL Backend.
- Moderne Datenbanken haben alle Voraussetzungen für unser Vorhaben.



Das **Backend** für die Authentifizierung

Der **Datensatz** im Backend wurde um ein paar Felder erweitert..

Field	Value	Comment
user	john.doe@domain.com	
password	anna69	
..	..	
mindiffsecs	15	min. Sekunden zwischen 2 Auth
maxipcount	3	max. Anzahl IP-Adressen in
iptimerange	1800	diesem Zeitraum
issmtp_in	TRUE	kann Mails empfangen
issmtp_out	TRUE	kann Mails versenden
isimap	TRUE	Zugriff auf Mails per IMAP
ispop3	FALSE	Zugriff auf Mails per POP3
is_only_de	FALSE	nur IP Adressen aus DE

Wir bringen eine SPAM Attacke über einen kompromittierten Account nach nur

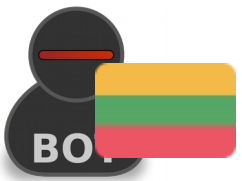
3 Mails

ohne manuellen Eingriff zum Erliegen.

Der Account wird nicht gesperrt,
das Passwort wird nicht geändert.

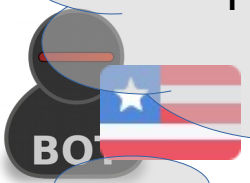
Hier haben wir das gegnerische Team der **SPAM** Attacke..

USER: john.doe@domain.com
PASSWORD: anna69

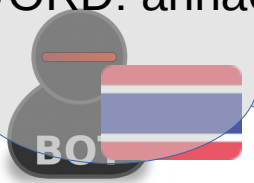


82.135.248.243

187.95.82.175



23.129.64.105

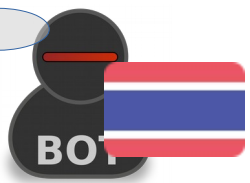


1.20.101.76

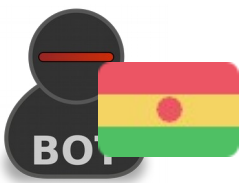
177.11.244.42

91.147.185.2

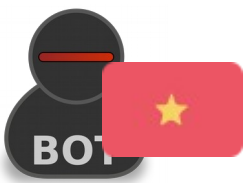
197.98.180.241



118.175.174.2



200.105.209.170

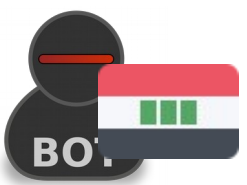


123.24.136.143

177.75.95.10

186.226.217.1

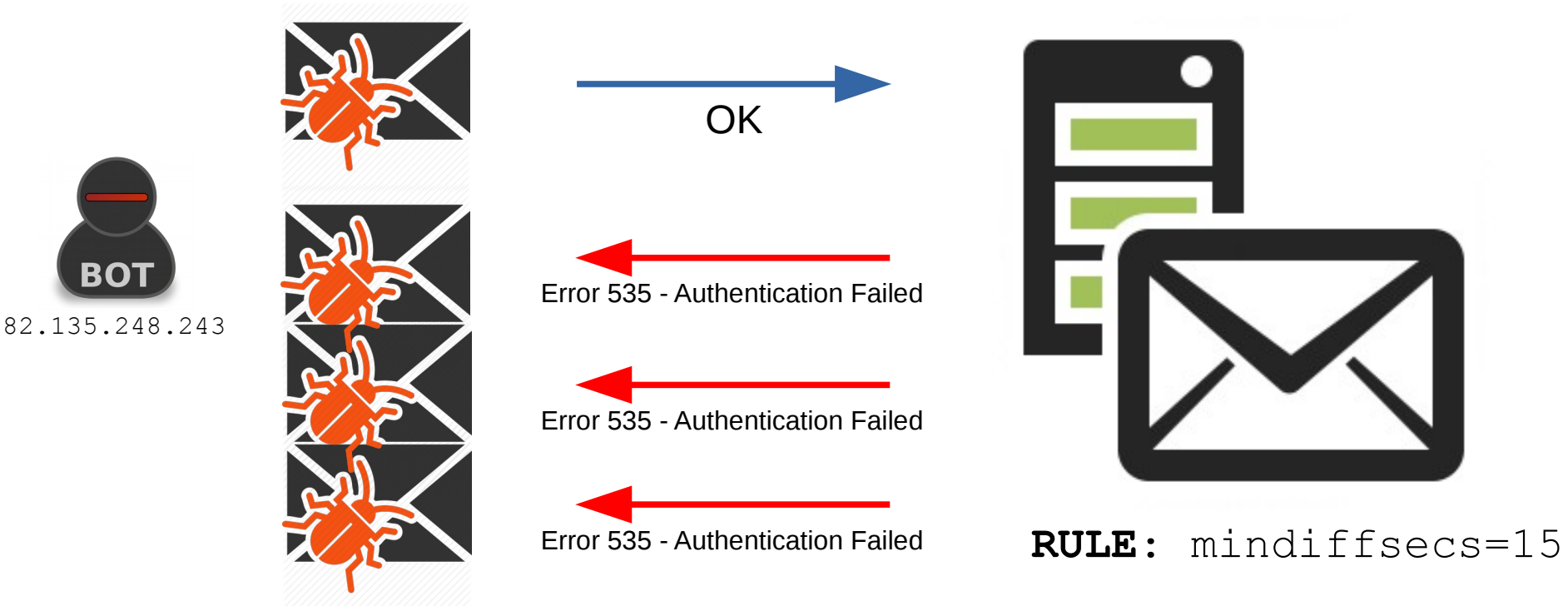
170.244.231.26



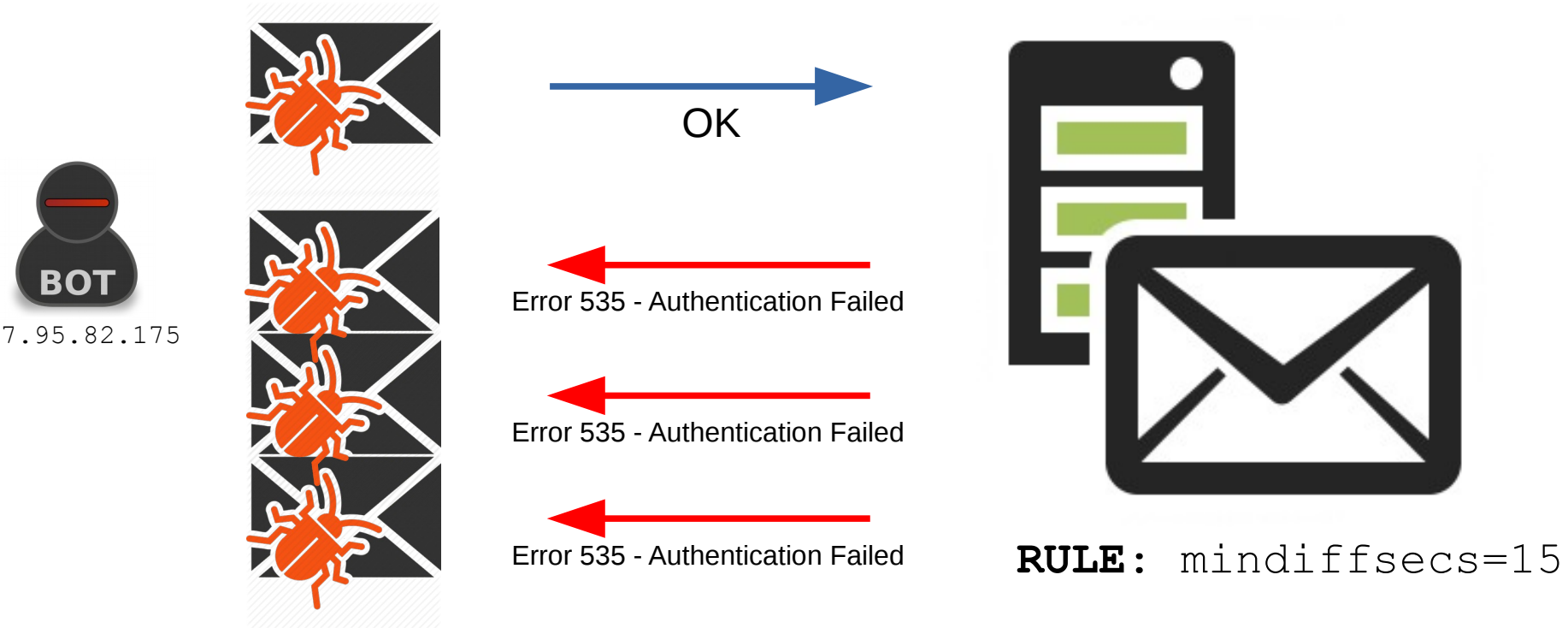
37.239.43.40

201.49.196.69

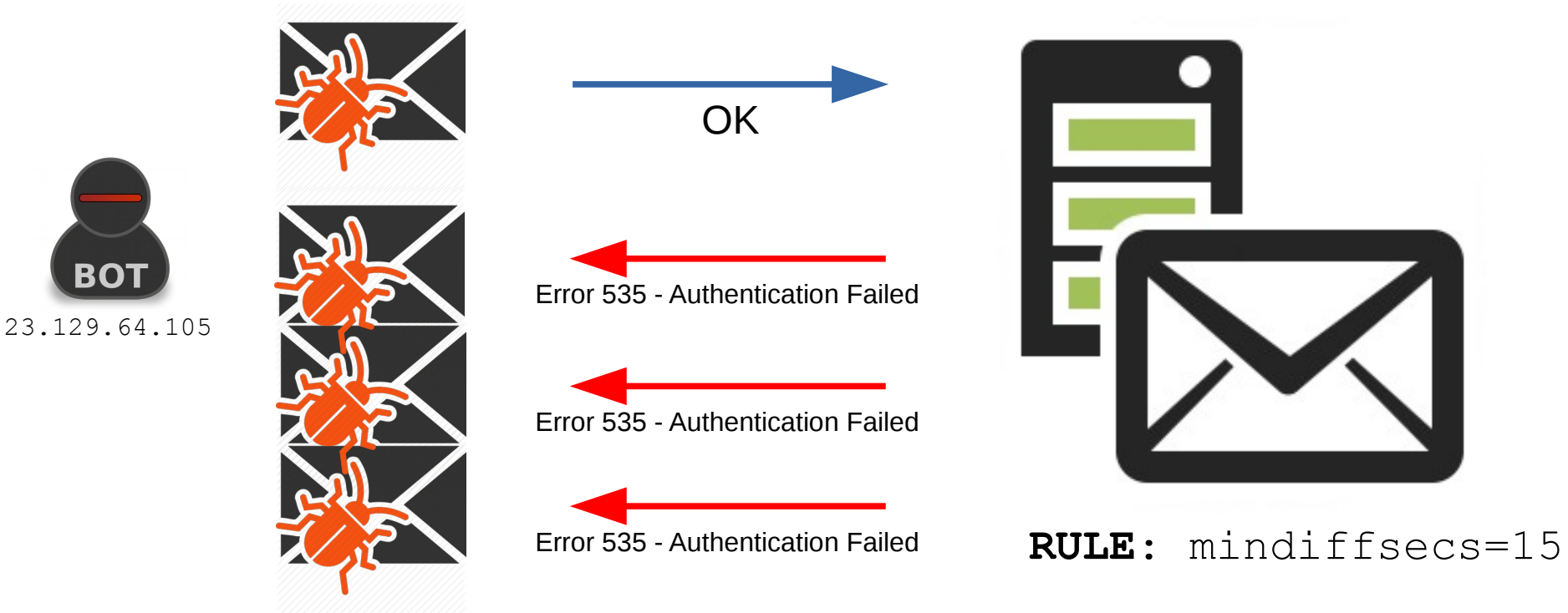
2018-12-18 13:49:41 Anstoß



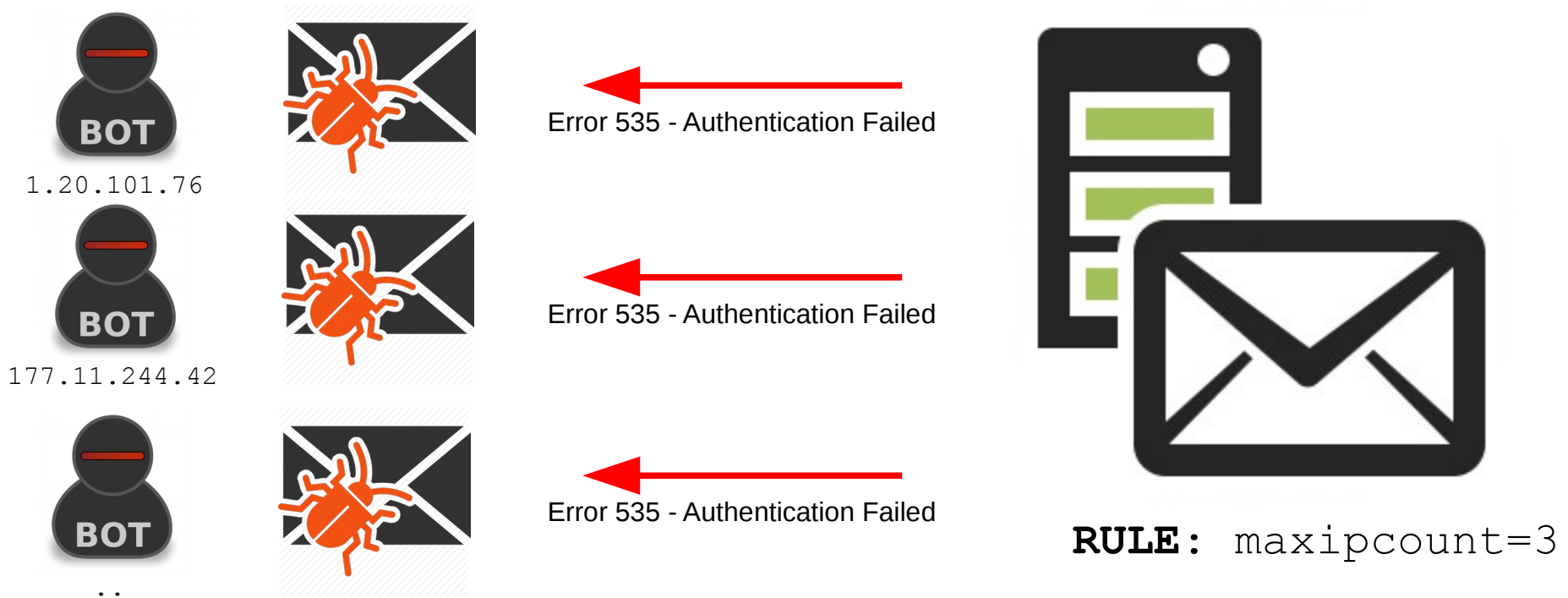
Der zweite **Player** : 2018-12-18 13:49:52



Der letzte **Player** mit einem Torschuss



Der **Rest** des Teams sieht nicht einmal den Ball..



So sieht die **SPAM** Attacke in der MySQL aus..

user	mailserver	ip	tstamp	blockedbytimediff	blockedbyipdiff
john.doe@domain.com	mx5.iunds.com	201.49.196.69	2018-12-18 13:52:51	NULL	2018-12-18 13:52:51
john.doe@domain.com	mx5.iunds.com	37.239.43.40	2018-12-18 13:52:42	NULL	2018-12-18 13:52:42
john.doe@domain.com	mx5.iunds.com	170.244.231.26	2018-12-18 13:52:25	NULL	2018-12-18 13:52:25
john.doe@domain.com	mx5.iunds.com	186.226.217.1	2018-12-18 13:52:17	NULL	2018-12-18 13:52:17
john.doe@domain.com	mx5.iunds.com	177.75.95.10	2018-12-18 13:51:59	NULL	2018-12-18 13:51:59
john.doe@domain.com	mx5.iunds.com	123.24.136.143	2018-12-18 13:51:55	NULL	2018-12-18 13:51:55
john.doe@domain.com	mx5.iunds.com	200.105.209.170	2018-12-18 13:51:23	NULL	2018-12-18 13:51:23
john.doe@domain.com	mx5.iunds.com	118.175.174.2	2018-12-18 13:50:57	NULL	2018-12-18 13:50:57
john.doe@domain.com	mx5.iunds.com	197.98.180.241	2018-12-18 13:50:56	NULL	2018-12-18 13:50:56
john.doe@domain.com	mx5.iunds.com	91.147.185.2	2018-12-18 13:50:37	NULL	2018-12-18 13:50:37
john.doe@domain.com	mx5.iunds.com	177.11.244.42	2018-12-18 13:50:35	NULL	2018-12-18 13:50:35
john.doe@domain.com	mx5.iunds.com	1.20.101.76	2018-12-18 13:50:12	NULL	2018-12-18 13:50:12
john.doe@domain.com	mx5.iunds.com	23.129.64.105	2018-12-18 13:50:03	2018-12-18 13:50:03	NULL
john.doe@domain.com	mx5.iunds.com	187.95.82.175	2018-12-18 13:49:52	2018-12-18 13:49:52	NULL
john.doe@domain.com	mx5.iunds.com	82.135.248.243	2018-12-18 13:49:41	2018-12-18 13:49:41	NULL

TÜV NORD CERT
DIN EN ISO 9001:2015

So sehen die

Ergeb-nisse

nach 18 Monaten aus

- Der technologische Ansatz funktioniert und wird vom Benutzer akzeptiert.
- Der Versuch solcher SPAM Attacken ist stark rückläufig. Unsere SMTP Server werden für Outbound SPAM uninteressant.
- Die Reputation der Mailserver ist so gut wie noch nie vorher!
- Die Technologie ist durch den Einsatz von Stored Procedures performant und skaliert sehr gut.
- Der administrative Aufwand in diesem Bereich beschränkt sich auf Statistik.

Wir

bauen weiter

- Der Wechsel von Passwörtern wird durch das Backend als gleitender Übergang zwischen Alt/Neu gestaltet.
- Die Anbindung des eigenen dynDNS Servers ermöglicht es die Herkunft von „Machine Accounts“ noch weiter einzuschränken.

Ich bedanke mich für Ihre

Aufmerksamkeit.
Fragen?
Antworten!

IUNDS

Zossener Straße 56-58
10961 Berlin

fon 030 – 20 61 59 30
s.illner@iunds.com

www.iunds.com