



**ZiM**

Zentrum für  
Informations- und  
Mediendienste

EUROPÄISCHER  
MONAT  
DER CYBER-  
SICHERHEIT

## ***Security-Check „E-Mail“***

UNIVERSITÄT  
DUISBURG  
ESSEN

*Offen im Denken*

 Rainer Pollak ■ 13.10.2017 14:00 Uhr

# Übersicht

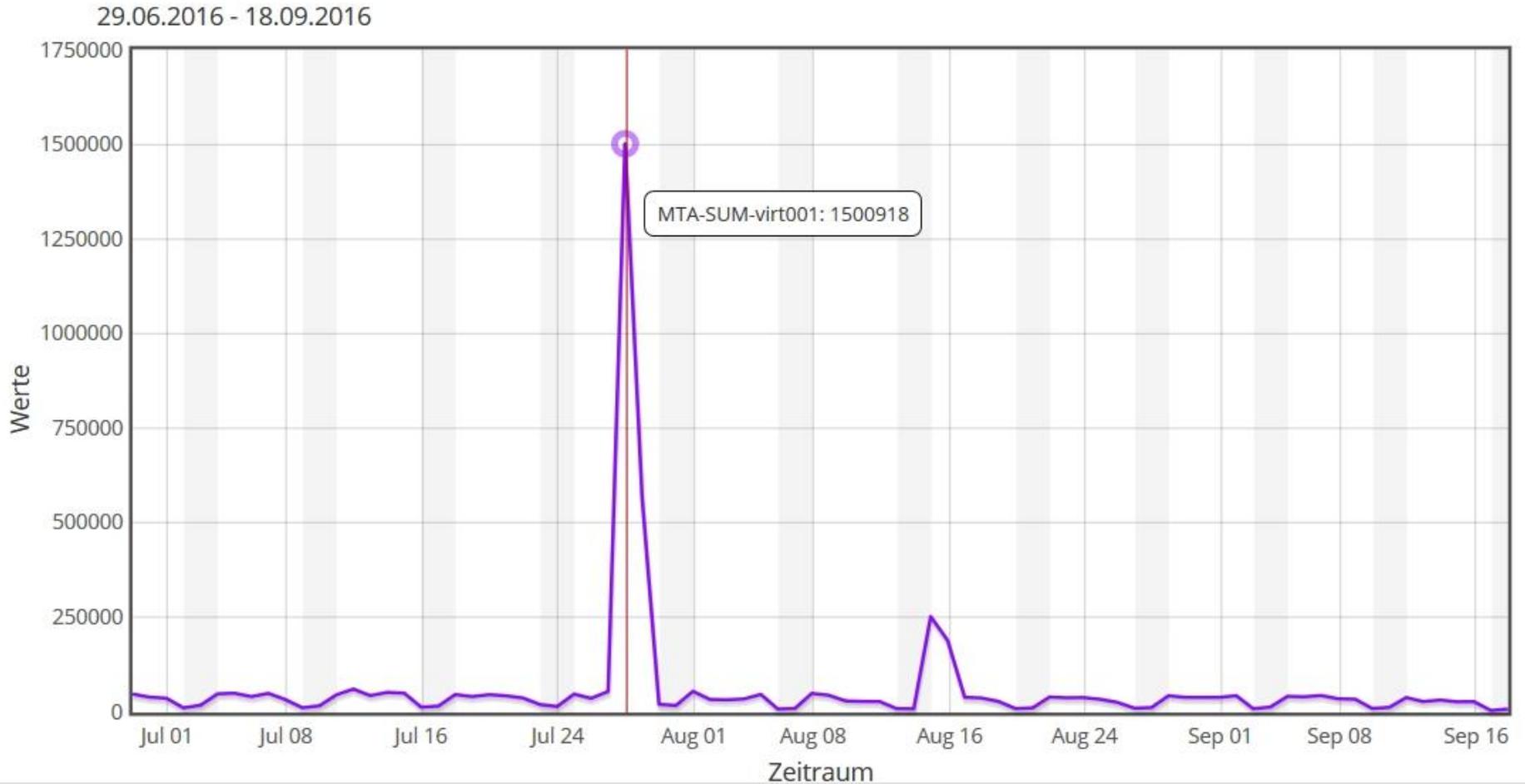
1. Einleitung
2. Technischer Spamschutz
  - Benutzerportal
  - Zahlen und Fakten
3. „Menschlicher“ Spamschutz
  - Aufbau einer URL
  - Drei-Punkte-Regel
  - Analyse von Phishing-Mail-Beispielen
4. S/MIME-Zertifikate
  - Authentizität, Integrität und Vertraulichkeit
  - Signierte E-Mails erkennen

# 1. Einleitung



UNIVERSITÄT  
DUISBURG  
ESSEN

*Offen im Denken*



- **Ziele und Schäden eines Angriffs auf die UDE:**
  - **Nutzung der breitbandigen Datenanbindung und der IT-Systeme: (D)DOS-Attacken, Systemscans, Spamverbreitung**
  - **Diebstahl von Forschungsdaten, Industriespionage**
  - **Finanzkriminalität**



UNIVERSITÄT  
DUISBURG  
ESSEN

*Offen im Denken*

## 2. „Technischer“ Spamschutz

## 2. Technischer Spamschutz



UNIVERSITÄT  
DUISBURG  
ESSEN

Offen im Denken



ZENTRUM FÜR INFORMATIONS- UND MEDIENDIENSTE

### Einstellungen für den Mailempfang

Diese Einstellungen werden auf dem zentralen Maileingangsserver ausgewertet, bevor eine E-Mail an das Postfach auf einem der Postfachserver weitergeleitet wird. Auf der Ebene des Postfaches können Sie weitere Einstellungen vornehmen, aber nicht die hier getroffenen Einstellungen ändern. Weitere Erläuterungen und Hinweise finden Sie unter [Schutz vor Viren, Malware etc.](#) .

### Wie soll bezüglich der SPAM-Abwehr verfahren werden?

Grundsätzlich gilt, dass eine aus irgend einem Grund abgewehrte Mail im technischen Sinne nicht angenommen wurde. Der absendende Mailserver konnte somit den Auftrag nicht erfüllen, die Mail erfolgreich zu übergeben. Ordentlich konfigurierte Mailserver informieren anschließend den Absender darüber, dass die E-Mail nicht zugestellt werden konnte.

- Kein Spamschutz: als SPAM erkannte E-Mails markieren und trotzdem zustellen.
- Mittlerer Spamschutz: als SPAM erkannte E-Mails nicht annehmen.
- Hoher Spamschutz: weitere Prüfungen durchführen und SPAM zurückweisen.

Wenn Sie hier keine Einstellung machen, gilt für Sie der mittlere Spamschutz.

### Greylisting

Mit Greylisting bieten wir ein Verfahren an, weitere Spammails zu erkennen und abzuwehren. Durch Greylisting kann es aber zu einer verzögerten E-Mail-Zustellung kommen.

- Greylisting erwünscht

### Behandlung einer E-Mail, in der ein Virus enthalten ist.

Zur Aufrechterhaltung der Betriebssicherheit wird eine E-Mail, die einen Virus enthält, grundsätzlich abgewehrt und von unseren Mailssystemen nicht angenommen.

- Ich möchte eine Benachrichtigung über das Abwehren der E-Mail erhalten

### Behandlung einer E-Mail, die einen ausführbaren Anhang enthält.

Zur Aufrechterhaltung der Betriebssicherheit wird eine E-Mail, die einen ausführbaren Anhang enthält, grundsätzlich abgewehrt und von unseren Mailssystemen nicht angenommen.

- Ich möchte eine Benachrichtigung über das Abwehren der E-Mail erhalten

Einstellungen

## 2. Technischer Spamschutz



EUROPÄISCHER  
MONAT  
DER CYBER-  
SICHERHEIT

UNIVERSITÄT  
DUISBURG  
ESSEN

*Offen im Denken*

### Kennungen und Wahl der Spamschutzstufen:

Kein Spamschutz: eigene Filterung	310	0,30 %
Mittlerer Spamschutz	101.722	99,57 %
Hoher Spamschutz	129	0,13 %
Summe:	102.161	100 %

Greylisting: 84

Stand: 04.10.2107

## 2. Technischer Spamschutz



UNIVERSITÄT  
DUISBURG  
ESSEN

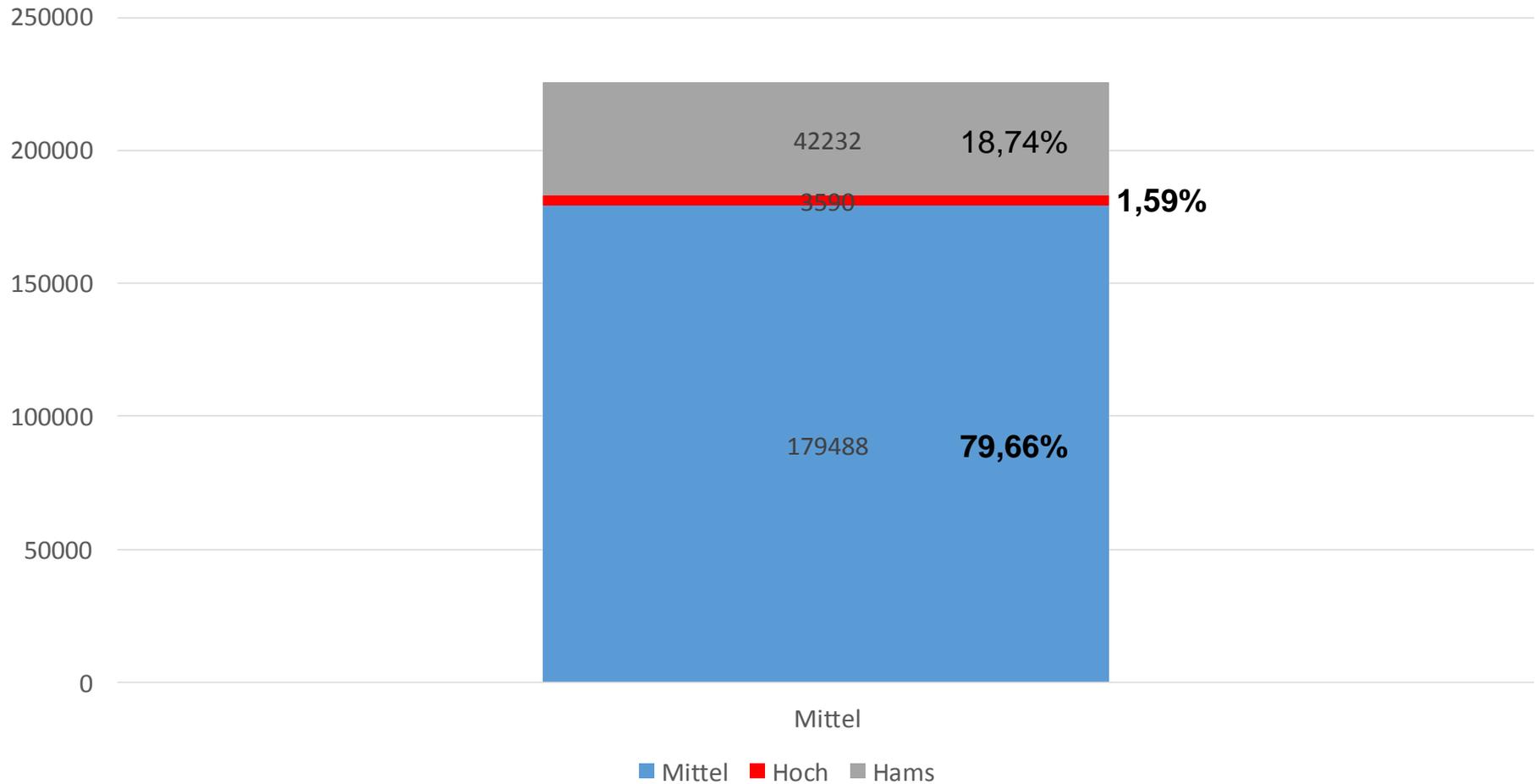
Offen im Denken

EUROPÄISCHER  
MONAT  
DER CYBER-  
SICHERHEIT

Empfänger

### Anteile Spams und Hams

03.10./04.10.2017





UNIVERSITÄT  
DUISBURG  
ESSEN

*Offen im Denken*

### 3. „Menschlicher“ Spamschutz

- Aufbau einer URL (Uniform Resource Locator)  
**https://webmail.uni-due.de/index.php**  
„Wer-Bereich“ (die Domain)
- Identifizierung der tatsächlichen Webadresse hinter einem Link:
  - Bereich zwischen „**http(s)://**“ und dem dritten Slash „**/**“
  - Betrachtung von rechts nach links:  
„de“ Punkt „uni-due“
  - Secure-HTTP mit gültigem Zertifikat!

### 3. „Menschlicher“ Spamschutz



EUROPÄISCHER  
MONAT  
DER CYBER-  
SICHERHEIT

UNIVERSITÄT  
DUISBURG  
ESSEN

Offen im Denken

- URL als IP-Adresse nicht vertrauenswürdig:  
<https://132.252.186.6/index.php> ❌
- Web-Ziel befindet sich nicht im „Wer-Bereich“:  
<http://campus.unidue.de.evil.com/lsf/rds?state=user> ❌  
<http://tamper.evil.com/campus.uni-due.de/lsf> ❌  
<https://campus.uni-due.de/lsf/rds?state=user&type=0> 😊
- Tippfehler, Buchstabendreher, ähnliche Zeichen und Auslassungen im „Wer-Bereich“:  
<http://benutzerverwaltung.uni-duisburg-essen.de/portal/> ❌  
<http://benutzerverwaltung.un-dujsburg-essen.de/portal/> ❌  
<https://benutzerverwaltung.uni-duisburg-essen.de/portal/> 😊

### 3. „Menschlicher“ Spamschutz



- „Wer-Bereich“ ist Abwandlung eines vertrauten Web-Ziels:  
<http://universitaet-duisburg-essen.de/> ❌
- Tipp:  
<https://whois.domaintools.com>

- **„3-Punkte-Regel zur Spamerkennung**
  - 1. Analyse der E-Mail-Kopfzeilen**
  - 2. Prüfung des E-Mail-Body**
  - 3. E-Mail-Anhang vorhanden: gefährliches Format (z. B. Microsoft-Office-Dokument)?**

### 3. „Menschlicher“ Spamschutz



UNIVERSITÄT  
DUISBURG  
ESSEN

Offen im Denken

## • Beispiel 1: gute oder böse E-Mail?

### IT-Support-Team



Von ZIM-Support   
An Pollak, Rainer   
Datum Mi 10:29

ziemm@uni-due.de

rainer.pollak@uni-due.de

Mit der Stärkung unseres Sicherheitssystems und der Verbesserung Ihrer Mailing-Erfahrung haben wir festgestellt, dass Ihre E-Mail-Einstellungen veraltet sind. Um die Sicherheit des Computersystems zu verbessern und die Anforderungen an die Bundesrechnungen zu erfüllen, benötigt ITS alle Sever-Benutzer, um ihr Konto zu aktualisieren, und klicken Sie auf [ITS](#), um Ihr Konto auf die neueste Outlook WebApp zu aktualisieren. Melden Sie sich an und aktualisieren Sie Ihre Mailbox automatisch, indem Sie die Anforderungen korrekt ausfüllen.

Vielen Dank  
Mit freundlichen Grüßen,  
ITS Service Desk

<http://itfreeservice.sitey.me/>

### 3. „Menschlicher“ Spamschutz



## • Beispiel 2: gute oder böse E-Mail?

### Zahlung\_06.10.2017



Von **Leiter des Instituts**   
An **Rainer Pollak**   
Datum **Mi 02:24**

Max.mustermann@uni-due.de

rainer.pollak@uni-due.de

Hallo!  
Können Sie eine internationale Banküberweisung heute nach Großbritannien machen?

[Rechnung](#)

Freundliche Grüße,  
Max Mustermann

<http://sciebo.unidue.de.fake.org/3sm28/Rechnung.xls>

### 3. „Menschlicher“ Spamschutz



## • Beispiel 3: gute oder böse E-Mail?

### Bewerbung als Buerokaufmann



Von Michael Hoffmann   
An Pollak, Rainer   
Datum Mi 11:32

hoffmann.michael@net-24.at

rainer.pollak@uni-due.de

### Bewerbung als Bürokaufmann

Sehr geehrter Herr Pollak,  
da ich auf der Suche nach einer neuen beruflichen Herausforderung bin, möchte ich mich hiermit bei Ihnen um eine Stelle als Bürokaufmann bewerben. Da ich bereits mehrere Jahre in diesem Bereich gearbeitet habe und zurzeit Arbeit suchend bin, möchte ich mich bei Ihnen bewerben.

Nach meiner Fachhochschulreife und meinen bisherigen Praktika konnte ich bereits Erfahrungen in unterschiedlichen Bereichen sammeln.

Sie finden in mir einen belastbaren, einsatzbereiten, flexiblen, selbstständigen und zuverlässigen Mitarbeiter mit hoher Teamorientierung. Das Einarbeiten in neue Aufgabengebiete bereitet mir keine Probleme.

Ich würde mich sehr freuen, wenn meine Bewerbung Ihr Interesse wecken konnte und ich mich persönlich bei Ihnen vorstellen darf. Über ein persönliches Gespräch freue ich mich sehr.

Mit freundlichem Gruß  
Michael Hoffmann

Anhang  
Lebenslauf und Arbeitszeugnis

<https://www.dropbox.com/sh/nzzv2i7/bewerb.doc>

[Dropbox-Download](#)

Die vollständige Bewerbungsmappe habe ich meine Dropbox geladen, weil die Datei für die Email zu groß war - Entschuldigen Sie bitte!

### 3. „Menschlicher“ Spamschutz



- **Problem: keine eindeutigen Zeichen für eine gefährliche E-Mail**
- **Weitere Schritte:**
  - **Datei-Download prüfen lassen:**  
**<https://virustotal.com>**
  - **Zeit verstreichen lassen; später wieder prüfen**
  - **Rückfrage an den Absender stellen**
  - **Falls „Expertenwissen“ vorhanden ist:**  
**Studium der Envelope-Header-Zeilen**
  - **Anfrage beim ZIM starten**



UNIVERSITÄT  
DUISBURG  
ESSEN

*Offen im Denken*

## 4. S/MIME-Zertifikate

- **Vorteile: Authentizität, Integrität und Vertraulichkeit**
- **Das ZIM kann S/MIME-Zertifikate für das Signieren und Verschlüsseln von E-Mails ausstellen.**
- **Das persönliche Zertifikat kann in die gängigen E-Mail-Programme wie Outlook, Thunderbird oder Evolution (Linux) eingebunden werden.**
- **Anleitungen:**  
<https://www.uni-due.de/zim/services/e-mail/konfigurationsanleitungen/zertifikat-anfordern.shtml>

## 4. S/MIME-Zertifikate



UNIVERSITÄT  
DUISBURG  
ESSEN

Offen im Denken



Pollak, Rainer

S/MIME-Zertifikate erhöhen die Sicherheit bei der E-Mail-Kommunikation

An Pollak, Rainer

Signiert von rainer.pollak@uni-due.de



### Sichere signierte und verschlüsselte E-Mails

Eine E-Mail ist technisch vergleichbar mit einem gewöhnlichen Brief. Die Absenderadresse wird sowohl bei einem Brief, als auch bei einer E-Mail sicherzustellen, dass eine E-Mail wirklich von einem bestimmten Absender auf dem Transportweg verfälscht worden ist, bietet sich der Einsatz einer digitalen Signatur, vergleichbar mit einer Unterschrift, an. Die elektronische Signatur wird durch ein persönliches Zertifikat des Versenders erzeugt.

**Digitale Signatur: Gültig** ✕

Betreff: S/MIME-Zertifikate erhöhen die Sicherheit bei der E-Mail  
Von: Pollak, Rainer  
Signiert von: rainer.pollak@uni-due.de

 Die digitale Signatur dieser Nachricht ist gültig und vertrauenswürdig.  
Klicken Sie auf "Details", um weitere Informationen zum Zertifikat zu erhalten, das für die digitale Signatur der Nachricht verwendet wurde.

Vor Fehlern in digital signierten Nachrichten vor dem Öffnen warnen.

[Details...](#) [Schließen](#)

Ende



UNIVERSITÄT  
DUISBURG  
ESSEN

*Offen im Denken*

**Vielen Dank!**  
**Fragen?**

- 10.10.2017 - Andreas Michels  
**Mit Sicherheit am Windows-Rechner - aber wie?**
- 13.10.2017 – Rainer Pollak  
**Security-Check „E-Mail“**
- 17.10.2017 – Dr. Andreas Bischoff  
**Der Kulturbeutel für das mobile Internet –  
sicher unterwegs mit Smartphone und Tablet**
- 20.10.2017 – Dr. Marius Mertens  
**Phishers Fritze phisht...**