TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

Informationsveranstaltung für Administratorinnen und Administratoren

Sachgebiet Informationssicherheit, TUD-CERT

Dresden, 20.05.2021

Agenda

- IT-Dokumentation aus Sicht der Informationssicherheit (Matthias Rack)
- Stand und Ausblick Nutzer- (und Serverzertifikate) (Matthias Rack)
- Stand Phishing-Training und Melde-Plugin (Pascal Brückner)
- Rückblick auf Teststellungen zu Sicherheit auf Endgeräten (Viviane Zenner)
- Löschfristen für personenbezogene Daten (Philipp Krahn, Jens Syckor)
- GSM: praktische Hinweise (Norman Walther)

TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

IT-Dokumentation an der TU Dresden aus Sicht der Informationssicherheit

Admin-Veranstaltung

Matthias Rack

Dresden, 20.05.2021

Durchführung und Ergebnis Pilotprojekt mit Fakultät EuI

- Initiative des ehemaligen Dekans der Fakultät EuI (heutigen CTIO), Wunsch nach Verbesserung der operativen Informationssicherheit
- Audit zum Status Quo durch SG 3.5 / TUD-CERT
- wichtiges Ergebnis: IT-Dokumentation an der Fakultät ist sehr heterogen
- Ergebnis lässt sich auf die TU Dresden übertragen

Erzeugt erhebliche Risiken:

- schnelle Handlungs- und Reaktionsfähigkeit im IT-Notfall nicht immer gegeben
- Notbremse: Abschaltung von IT-Ressourcen bzw. von Struktureinheiten bei Sicherheitsvorfällen
- kann im Extremfall zur Handlungsunfähigkeit der Universität führen

Aktueller Stand und Planung

- Katalog mit Mindestanforderung an IT-Dokumentation (in Zusammenarbeit mit Administrator der Professur für Schaltungstechnik und Netzwerktheorie)
- Prototypische Umsetzung, aber technische Grenzen
- Abstimmung zwischen CDIO und SG 3.5 zur Finalisierung der Mindestanforderungen und zur Anpassung des IT-Bestandsportals

Nächste Schritte:

- Thema in AG Datenschutz und Informationssicherheit
- Anpassung des IT-Bestandsportals mit ausgewählten Attributen aus Mindestanforderung
- Welche Tools unterstützen die automatisierte IT-Dokumentation und können TU-weit und einheitlich eingesetzt werden?
- Folgerung: Aufsetzen eines Projekts zur IT-Dokumentation

TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

Stand und Ausblick Nutzer- (und Serverzertifikate)

Admin-Veranstaltung

Matthias Rack

Dresden, 20.05.2021

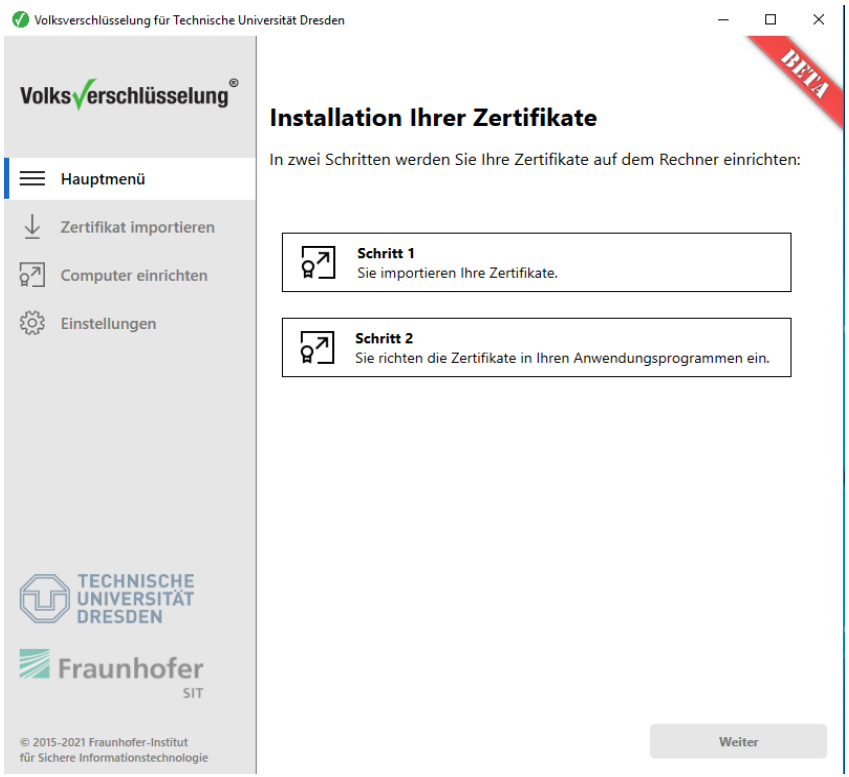
Aktueller Stand EVAZert

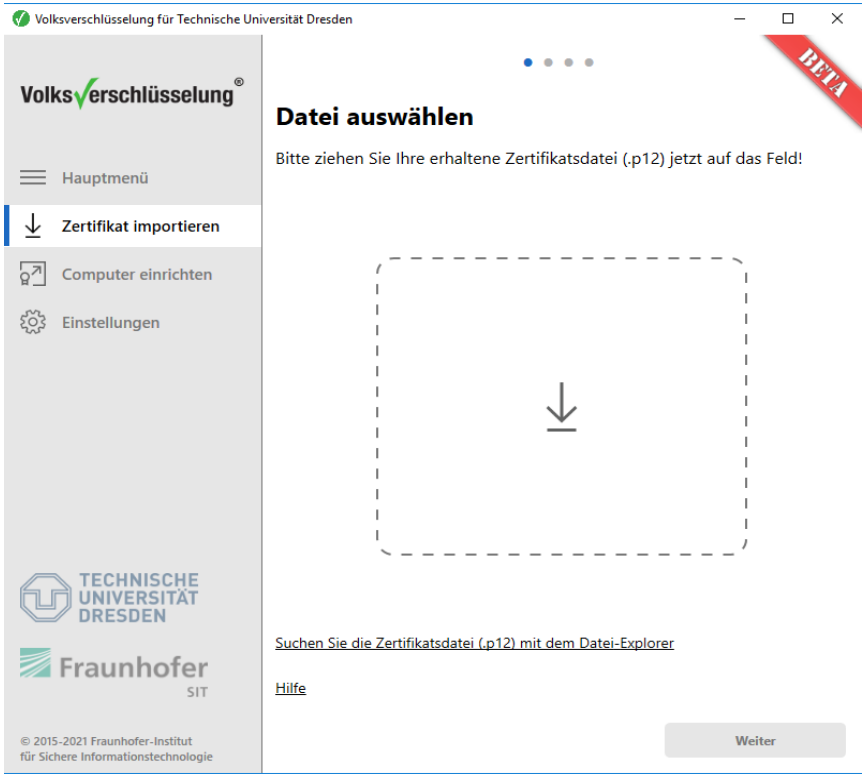
- Prozess seit 02/2020 universitätsweit etabliert
- technische und organisatorische Maßnahmen zur Erleichterung von Beantragung und Nutzung digitaler Zertifikate aus der DFN-PKI
- jede neue Mitarbeiterin / jeder neue Mitarbeiter erhält bei Einstellung ein S/MIME-Zertifikat
- Statistik:
    - derzeit 61 prüfberechtigte Personen (inkl. Service Desk)
    - Anträge über EVAZert gesamt: 2307
    - aktive Zertifikate: 2035

VV-App (TUD Edition) I

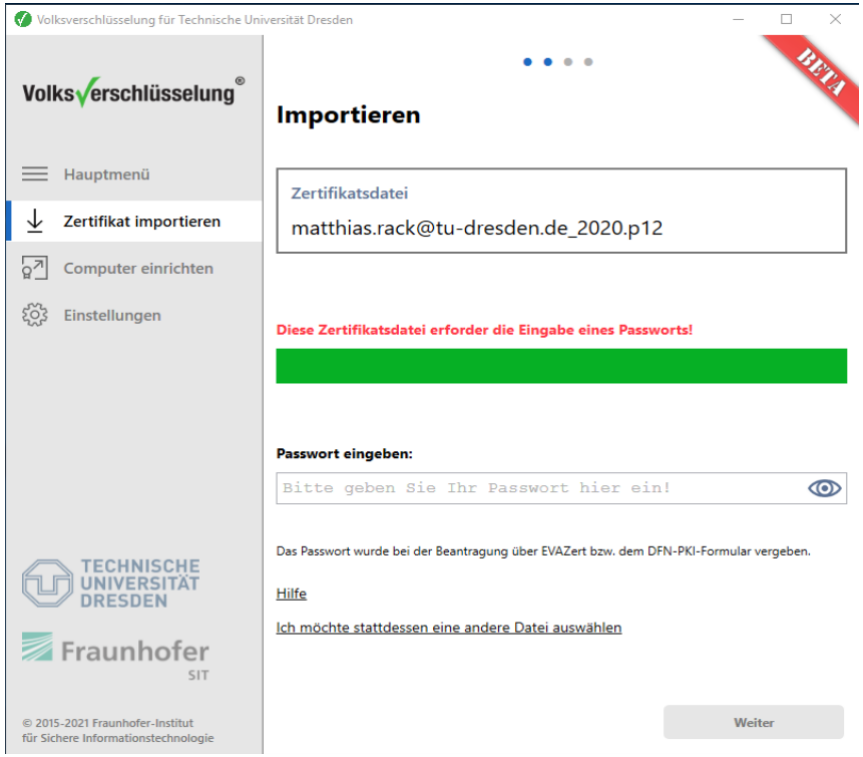
- Einsatz der VV-App-Technologie (Key2B) des Fraunhofer SIT, Darmstadt
- Installation der App über Software-Verteilungssysteme oder manuell
- .p12-File wird in alle vorhandenen Zertifikatsspeicher importiert (unter MS Windows): Outlook, Thunderbird, Adobe Acrobat etc.
- Software, die mit digitalen Zertifikaten operiert, wird automatisch konfiguriert
- administrativer Aufwand bei Zertifikatsinstallation und -konfiguration wird verringert

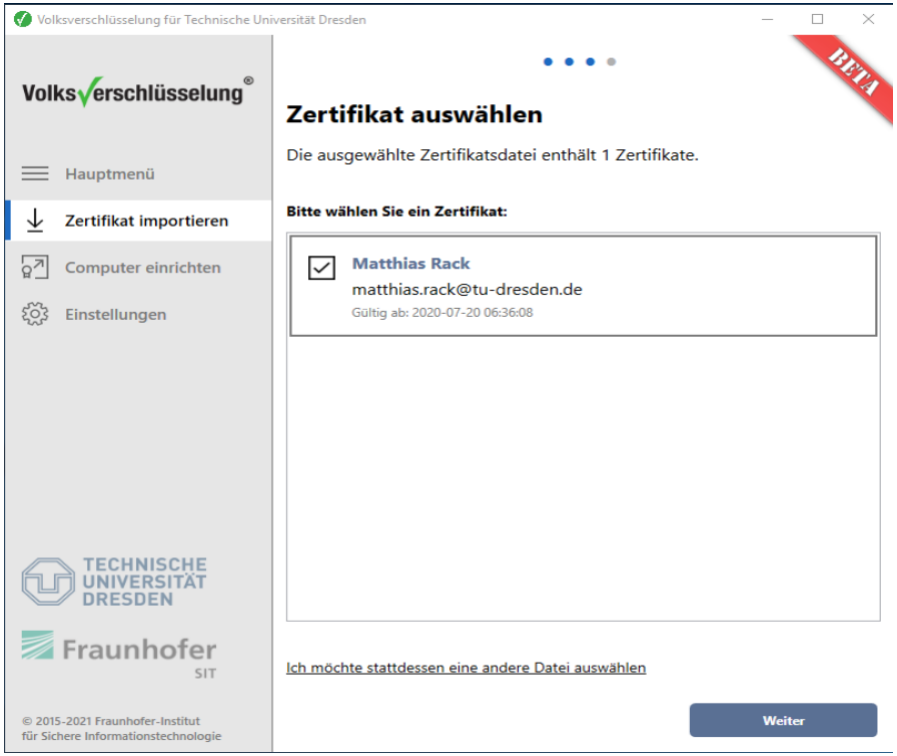
VV-App (TUD Edition) II



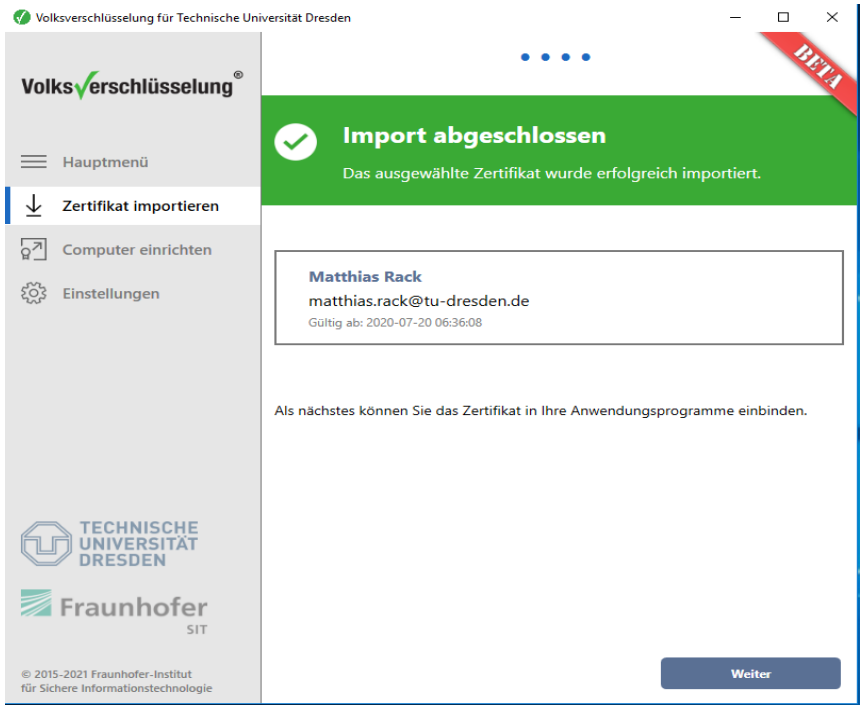


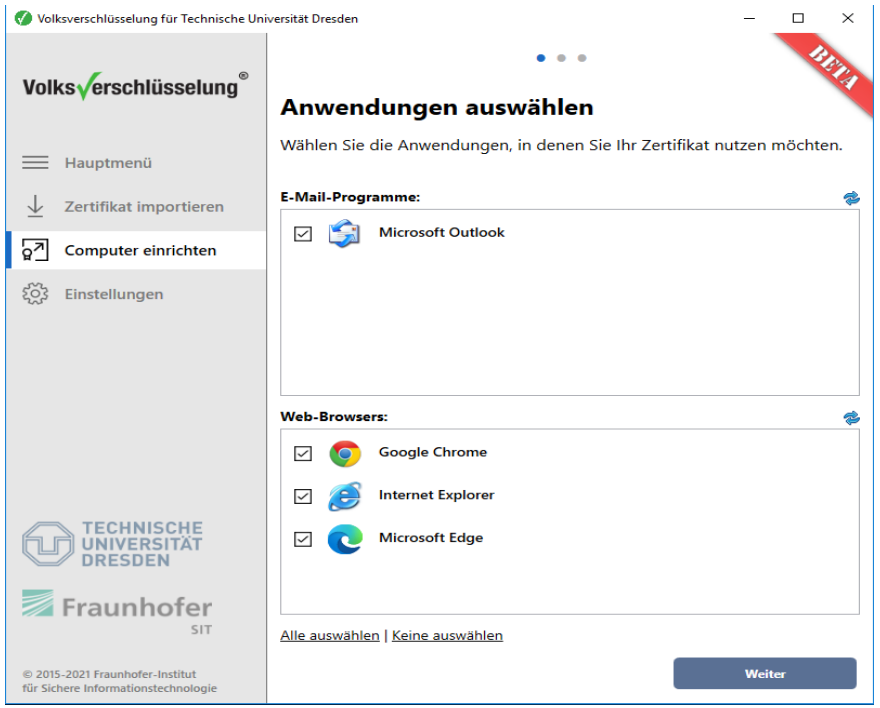
VV-App (TUD Edition) III



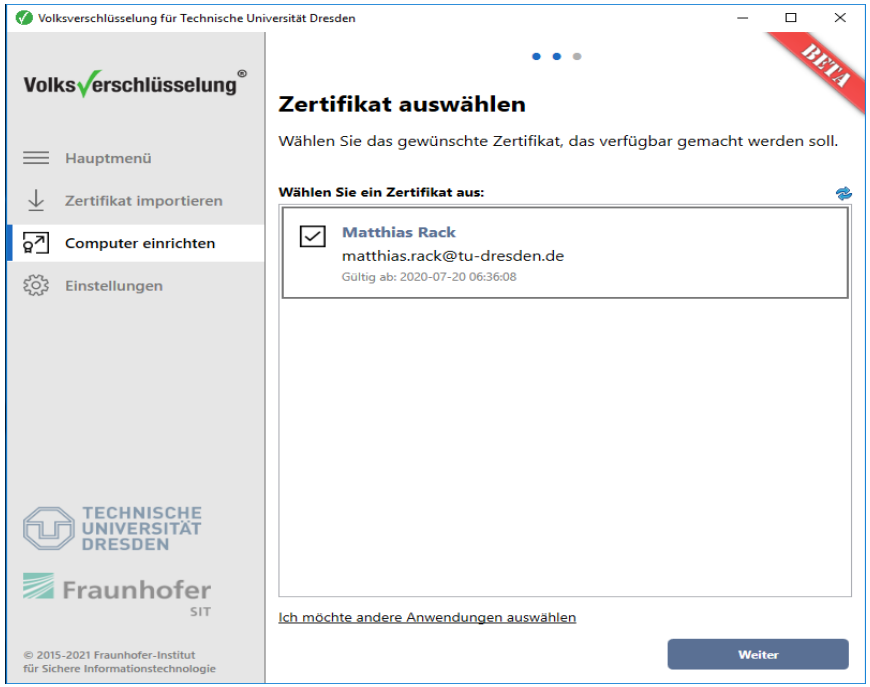


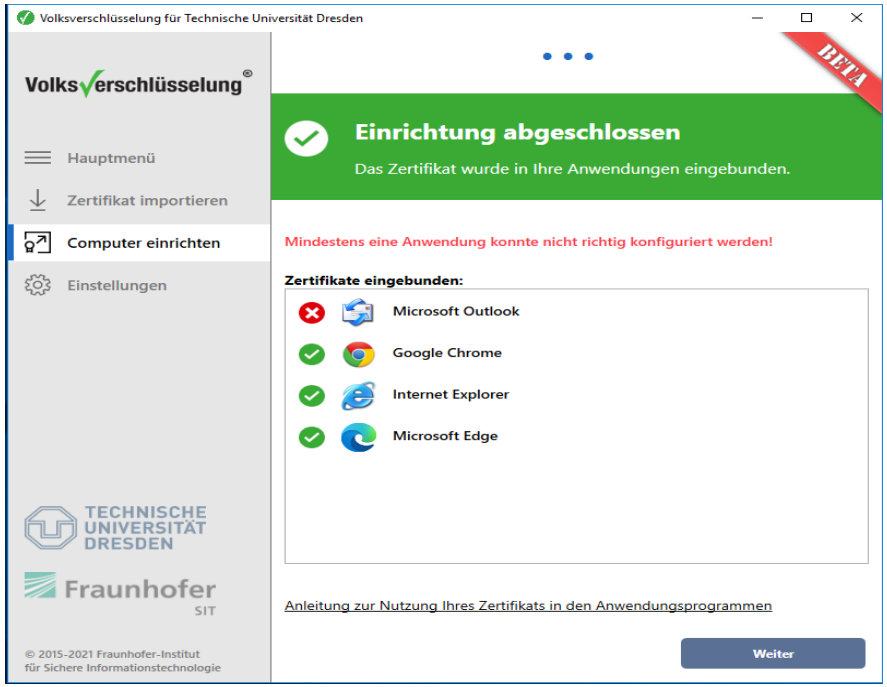
VV-App (TUD Edition) IV





VV-App (TUD Edition) V





Planung und Ausblick

- Einsatz des Trusted Certificate Service (TCS) von GÉANT - Bereitstellung durch DFN
- Ausstellung von Nutzerzertifikaten nach SAML-Authentifizierung über die DFN-AAI/eduGAIN ohne papierbasierte Antragsformulare
- keine Identitätsprüfung mit Lichtbild-Ausweis mehr nötig
- damit können potentiell alle Studierenden S/MIME-Zertifikate erhalten
- Umsetzung ist für 2021 geplant / TU Dresden bereits im frühen Pilotbetrieb - „alte Welt“ der DFN-PKI im Hinblick auf Nutzerzertifikate existiert aber weiter
- Unterstützung des ACME-Protokolls für das vollautomatisierbare Deployment von organisationsvalidierten Serverzertifikaten

TECHNISCHE UNIVERSITÄT DRESDEN

TUD CERT Computer Emergency Response Team

Pascal Brückner
TUD-CERT

Phishing-Melde-Plugin

und integriertes Lernen am Arbeitsplatz

20.05.2021

Phishing-Simulation an der TUD
Aktueller Planungsstand

Zweck Sensibilisierung v. Nutzern mit simulierten Phishing-Angriffen per E-Mail

Inhalte Interne Dienste, aber auch “klassisches“ Phishing (Paypal/Gmail etc.)

Phishing-Simulation an der TUD
Aktueller Planungsstand

Zweck Sensibilisierung v. Nutzern mit simulierten Phishing-Angriffen per E-Mail

Inhalte Interne Dienste, aber auch “klassisches“ Phishing (Paypal/Gmail etc.)

Phishing-Server Externes Hosting, Umzug in Planung

Phishing-Simulation an der TUD
Aktueller Planungsstand

Zweck	Sensibilisierung v. Nutzern mit simulierten Phishing-Angriffen per E-Mail
Inhalte	Interne Dienste, aber auch “klassisches“ Phishing (Paypal/Gmail etc.)
Phishing-Server	Externes Hosting, Umzug in Planung
Umfang	Ausschließlich TUD-Angestellte, **keine** Gäste und Studierende (ca. 15k Personen)

Phishing-Simulation an der TUD
Aktueller Planungsstand

Zweck	Sensibilisierung v. Nutzern mit simulierten Phishing-Angriffen per E-Mail
Inhalte	Interne Dienste, aber auch “klassisches“ Phishing (Paypal/Gmail etc.)
Phishing-Server	Externes Hosting, Umzug in Planung
Umfang	Ausschließlich TUD-Angestellte, **keine** Gäste und Studierende (ca. 15k Personen)
Rechtliches	Dienstvereinbarung mit Personalrat beschlossen

Phishing-Simulation an der TUD
Aktueller Planungsstand

Zweck	Sensibilisierung v. Nutzern mit simulierten Phishing-Angriffen per E-Mail
Inhalte	Interne Dienste, aber auch “klassisches“ Phishing (Paypal/Gmail etc.)
Phishing-Server	Externes Hosting, Umzug in Planung
Umfang	Ausschließlich TUD-Angestellte, **keine** Gäste und Studierende (ca. 15k Personen)
Rechtliches	Dienstvereinbarung mit Personalrat beschlossen
Häufigkeit	Periodisch, etwa eine Mail pro Quartal
Start	Zunächst kleiner Kreis von Testnutzern, offiziell mit Beruhigung des Pandemiegeschehens

Phishing-Melde-Plugin
für Microsoft Outlook

Idee Unkomplizierte Meldemöglichkeit von potentiell gefährlicher E-Mails per Knopfdruck. Gemeldete E-Mails hängen der Meldung vollständig an (mit vollständigen Headern).

Phishing-Melde-Plugin
für Microsoft Outlook

Idee Unkomplizierte Meldemöglichkeit von potentiell gefährlicher E-Mails per Knopfdruck. Gemeldete E-Mails hängen der Meldung vollständig an (mit vollständigen Headern).

Zweck Meldung von Phishing, Scams und Mails mit schadhaften Anhängen. Normaler Werbespam sollte **NICHT** gemeldet werden.

Phishing-Melde-Plugin
für Microsoft Outlook

Idee Unkomplizierte Meldemöglichkeit von potentiell gefährlicher E-Mails per Knopfdruck. Gemeldete E-Mails hängen der Meldung vollständig an (mit vollständigen Headern).

Zweck Meldung von Phishing, Scams und Mails mit schadhaften Anhängen. Normaler Werbespam sollte **NICHT** gemeldet werden.

Prozess Meldungen erzeugen bei uns Tickets, wir prüfen und ergreifen ggf. Gegenmaßnahmen. Rückmeldung unsererseits nur falls weitere Informationen benötigt werden.

Phishing-Melde-Plugin
für Microsoft Outlook

Idee Unkomplizierte Meldemöglichkeit von potentiell gefährlicher E-Mails per Knopfdruck. Gemeldete E-Mails hängen der Meldung vollständig an (mit vollständigen Headern).

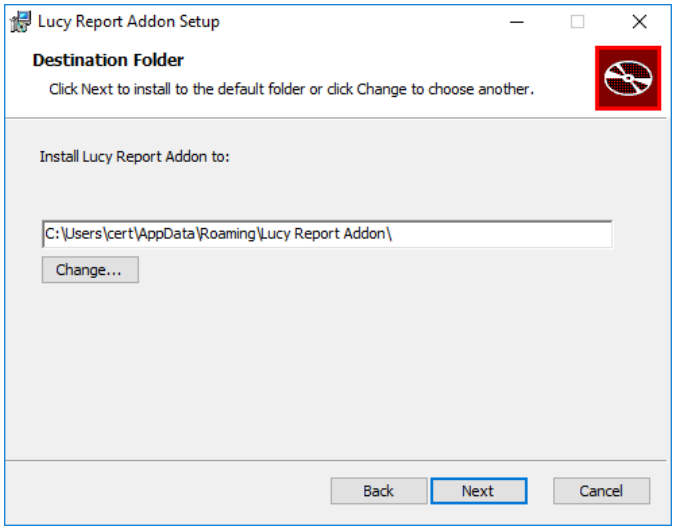
Zweck Meldung von Phishing, Scams und Mails mit schadhaften Anhängen. Normaler Werbespam sollte **NICHT** gemeldet werden.

Prozess Meldungen erzeugen bei uns Tickets, wir prüfen und ergreifen ggf. Gegenmaßnahmen. Rückmeldung unsererseits nur falls weitere Informationen benötigt werden.

Training Meldung aus Phishing-Simulation ebenfalls über das Plugin möglich, Phishing-Server ordnet diese laufenden Kampagnen automatisch zu. Manuelle Meldung via Weiterleitung an `cert-meldung@mailbox.tu-dresden.de` weiterhin möglich.

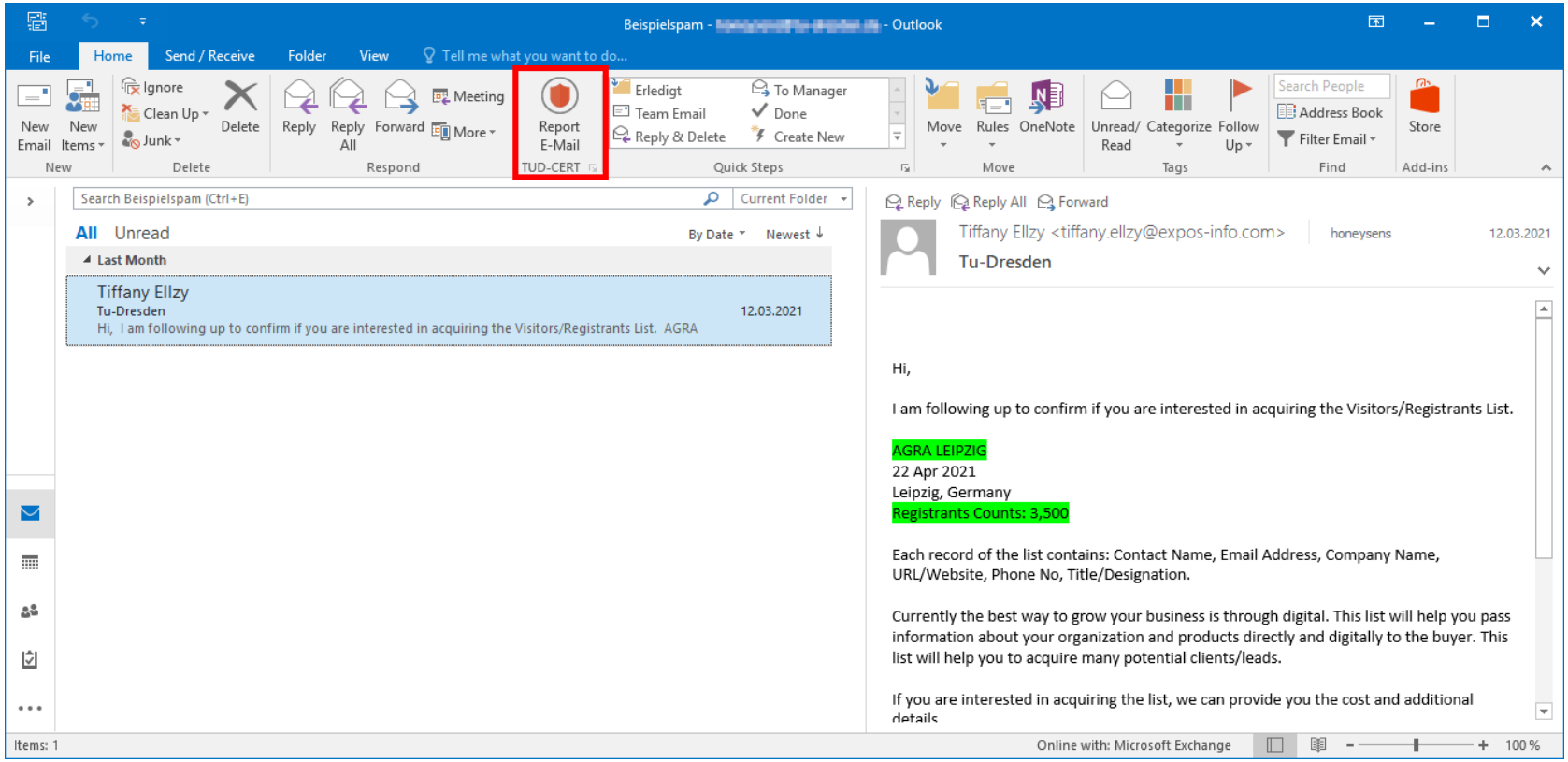
Funktionsweise Das Plugin ist Teil unserer Phishing-Software *Lucy*, Meldungen erzeugen SMTP und HTTPS-Verbindungen.

Phishing-Melde-Plugin
Installation

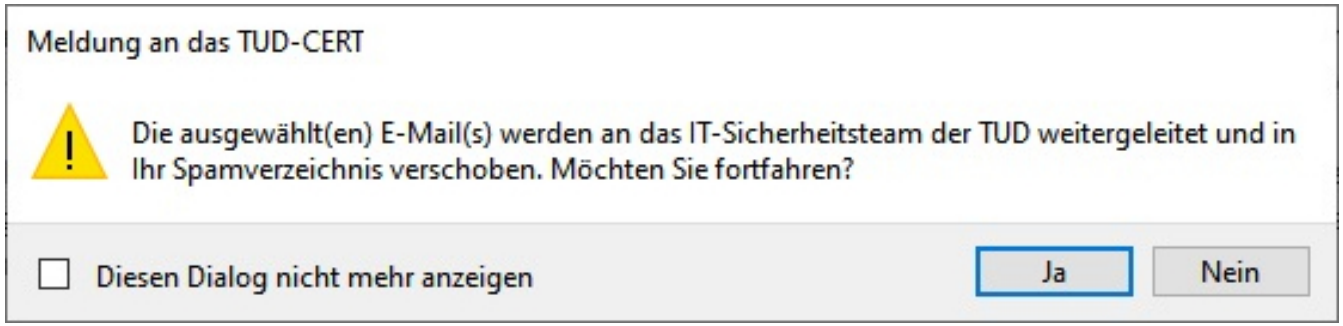


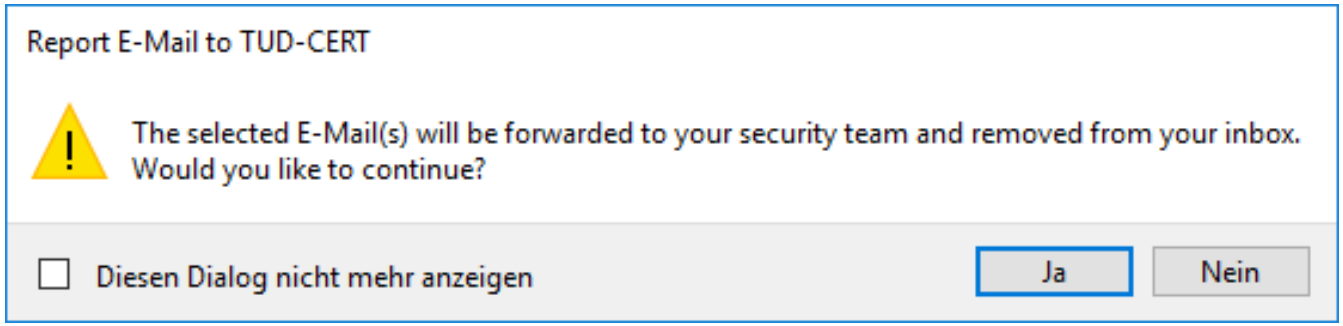
- Installation wahlweise für lokalen Benutzer oder systemweite (separate MSI)
- In AD-Domänen kann systemweiter Installer zentral verteilt werden

Phishing-Melde-Plugin
Outlook-Integration

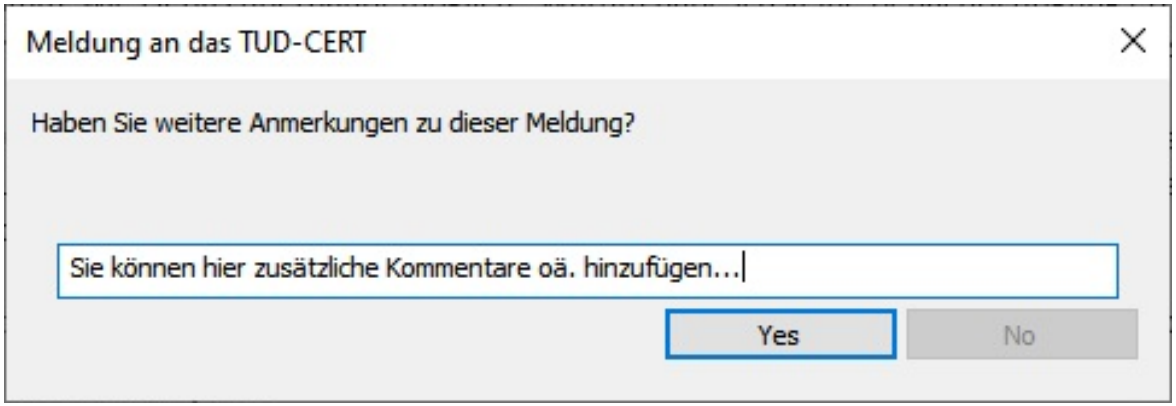


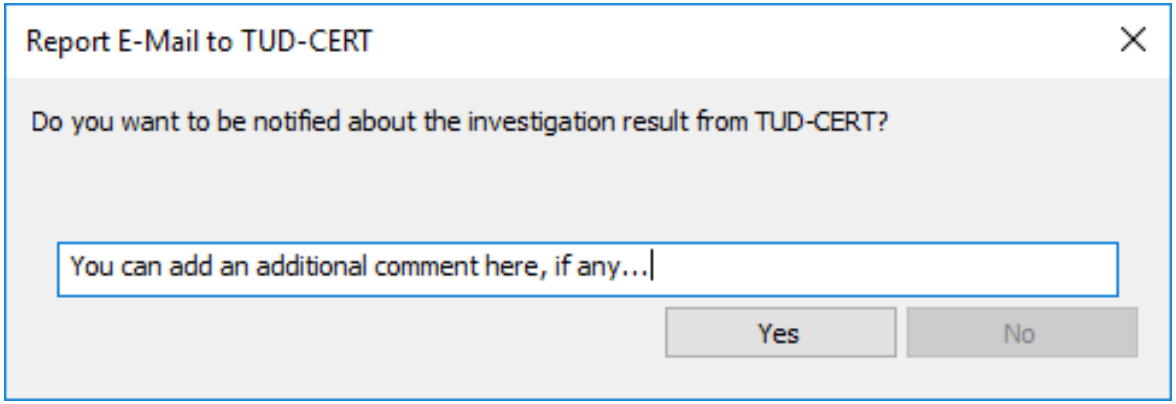
Phishing-Melde-Plugin
Meldeprozess (1)



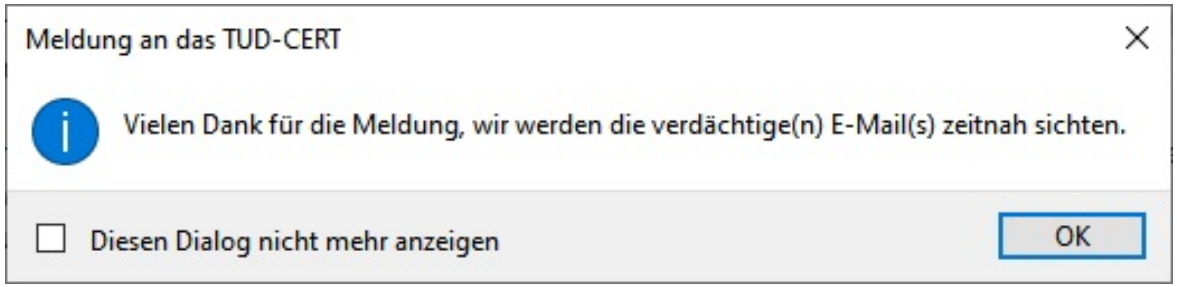


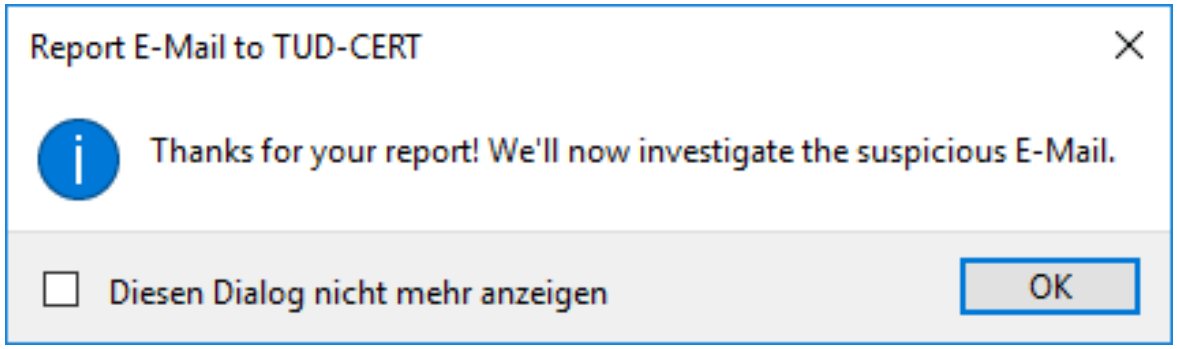
Phishing-Melde-Plugin
Meldeprozess (2)





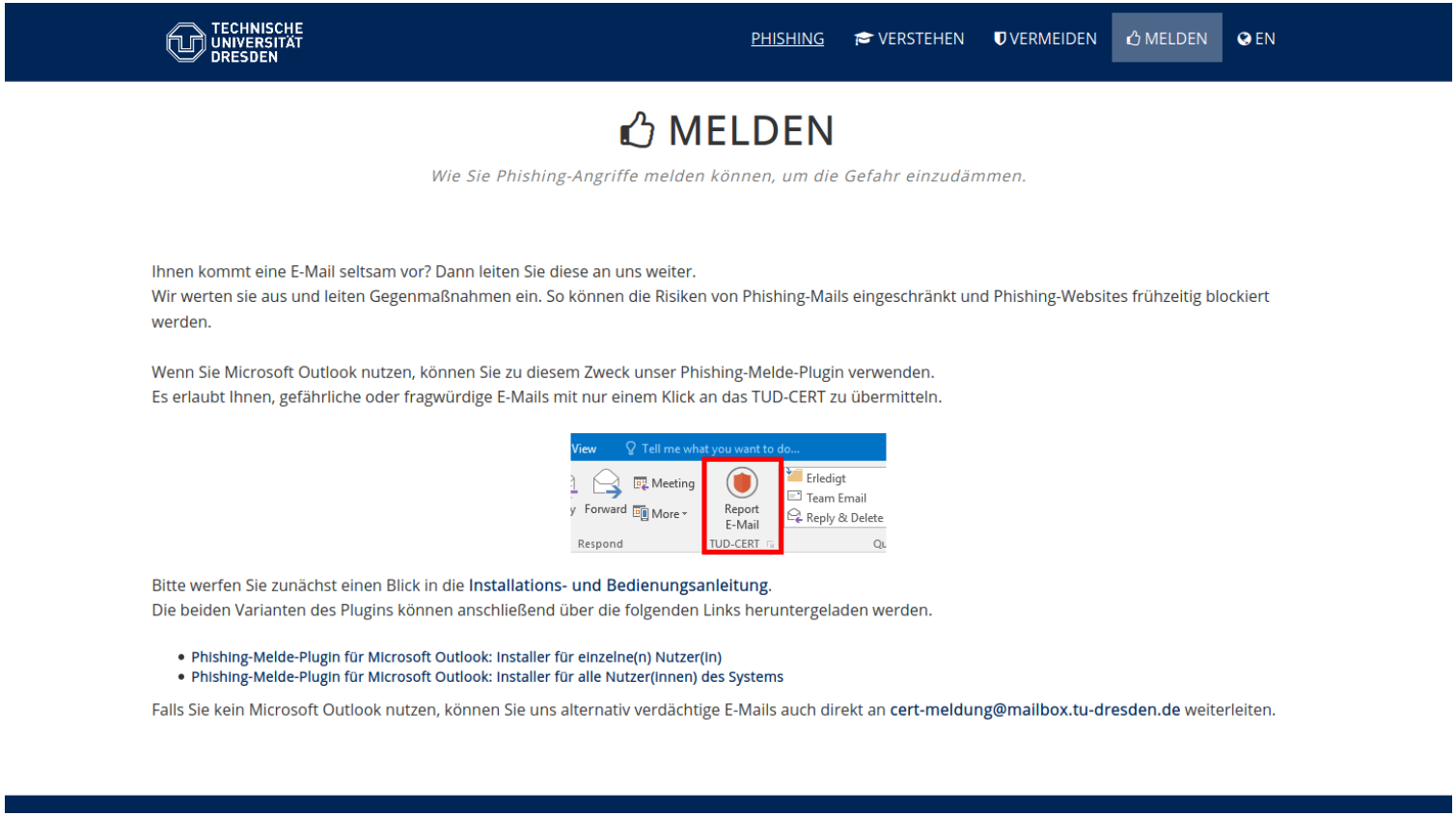
Phishing-Melde-Plugin
Meldeprozess (3)





Phishing-Melde-Plugin
Verfügbarkeit

- Download und Installation-/Bedienungsanleitung auf `https://mailsecurity.cert.tu-dresden.de`



TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

TUD CERT Computer Emergency **Response Team**

Proof of Concept - Endpointsecurity

Viviane Zenner, TUD-CERT, Sachgebiet Informationssicherheit

Dresden, 20.05.2021

Proof of Concept - Allgemeines

• Endpointsecurity – Dokumente und Webseiten in einer geschützten Umgebung öffnen

• eventuelle Schadsoftware in Dokumenten, bspw. aus Mailversand/Mailanhängen, wird in einer virtuellen Maschine (VM) und nicht auf dem Rechner ausgeführt – keine Gefahr für das Basis-System

• potentiell bösartige Links aus Spam- oder Phishing-Mails werden ebenfalls durch den Browser der geschützten Umgebung geöffnet (extra VM) und können das Basis-System nicht schädigen

• die VMs können dann ganz einfach wie ein normales Anwendungsfenster geschlossen/beendet werden

Proof of Concept - Allgemeines

- zwei Produkte wurden getestet
  - Browser in the Box von Rhode & Schwarz
  - HP Sure Click Enterprise
- jeder PoC lief über 4 Wochen
  - 10.03.2021 – 07.04.2021 (Bit Box)
  - 14.04.2021 – 12.05.2021 (HP Sure Click Enterprise)

Proof of Concept - Beteiligung

- Beteiligung bedingt durch Pandemie eingeschränkt
    - mobile Arbeit schränkt breiter aufgestellte Tests ein
    - Absprache und Problembewältigung eingeschränkt
- beide Produkte wurden auf ca. 10 - 15 Clients getestet
- Feedbacks aufgrund eingeschränkter Testmöglichkeiten entsprechend gering, aber Tendenzen klar erkennbar

Proof of Concept - Feedback

Bit Box & Document Viewer

- fehlende Installationshinweise sorgten teilweise für mehrere Probleme

- da kein NAT zwischen den Clients und dem Web-Gateway möglich ist, wird ein Rollout eher problematisch

- Einschränkungen im Arbeitsablauf:
  - keine Möglichkeit für Videokonferenzen
  - keine Speicherung von Cookies
  - schlechte Downloadgeschwindigkeit
  - keine Funktionsfähigkeit ohne VPN
  - mehr Perfomance benötigt als bei anderen Browsern

Document Viewer:

- Darstellungsprobleme (nur bestimmte Formate geöffnet)
- Viewer nicht gefunden und daher nicht getestet

Proof of Concept - Feedback

HP Sure Click Enterprise

• durch Cloudvariante und gute Dokumentation verlief die Installation problemlos

• keine Meldungen von Teilnehmern über Probleme während des Tests

• keine Einschränkungen im Arbeitsablauf und keine Perfomanceprobleme

• nicht alle Dateien eines Formates (bspw. PDF) wurden erkannt

• Hinweise zum Öffnen durch den integrierten Browser wäre für nicht technisch-versierte Nutzer sinnvoll

• eine produktive Nutzung ist denkbar

Proof of Concept

Danke allen Teilnehmern für Ihre Mithilfe und Feedbacks!

Danke allen Zuhörer*innen für Ihre Aufmerksamkeit!

TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

Löschung von personenbezogenen Daten

Admin-Workshop (20.05.2021)

Philipp Krahn / stellv. DSB

Jens Syckor / DSB

informationssicherheit@tu-dresden.de

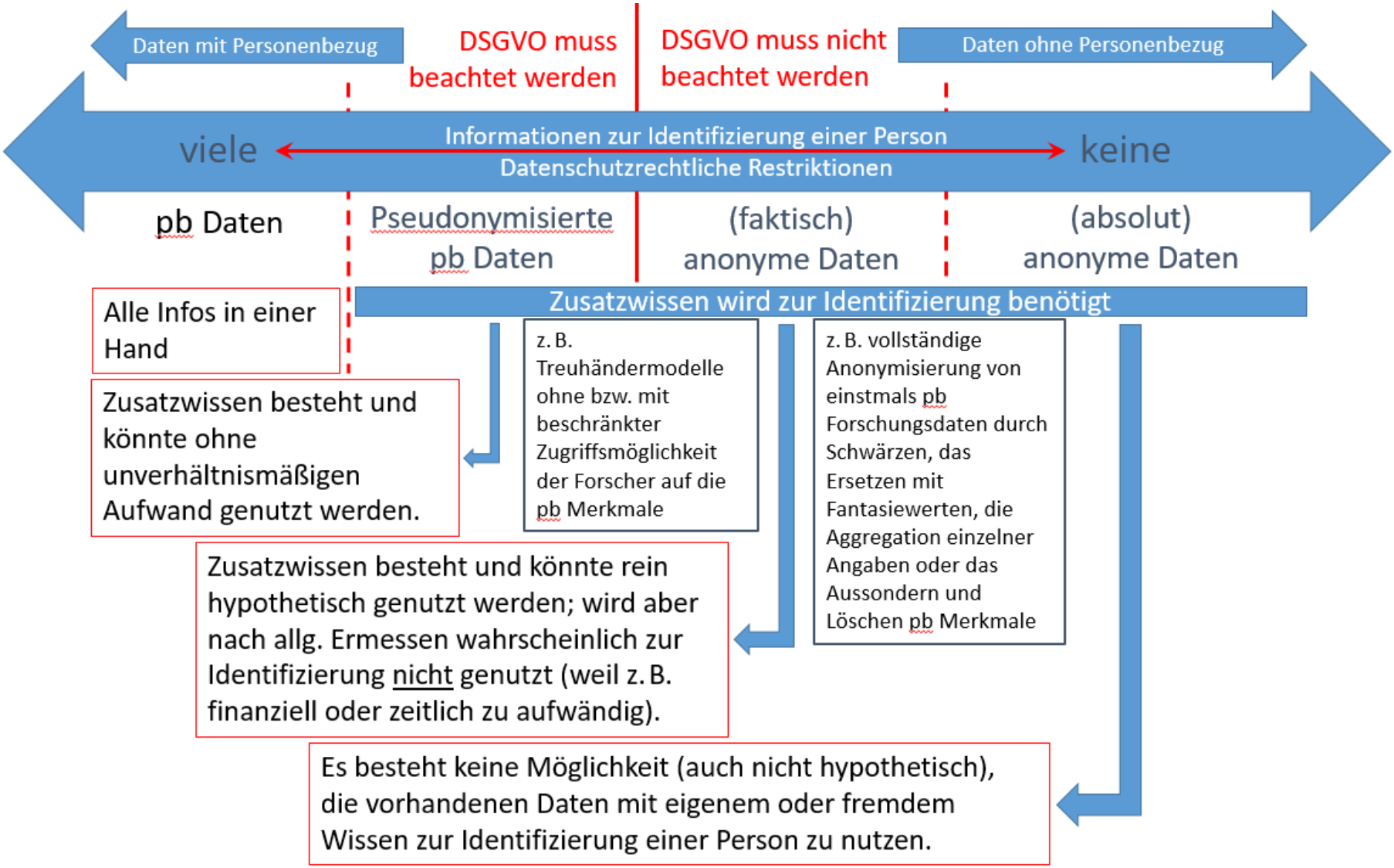
Grundlegende rechtliche Vorgaben zur Löschung

Art. 17 Abs. 1 lit. 1 DSGVO:

Der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sobald die „personenbezogenen Daten [...] für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig [sind]“.

- Die Löschung erfolgt i.d.R. durch die für die Datenverarbeitung zuständige Organisationseinheit oder Person und wird so durchgeführt, dass im Anschluss keine Rückschlüsse auf die Identität der betroffenen Person möglich sind.
- Stattdessen: Vernichtung (bei Akten) oder Anonymisierung (strittig, zumindest für Forschungs-, Statistik- oder Archivzwecke)

Anonymisierungsgrade



Fristen bis zur Löschung/Vernichtung/Anonymisierung

Die Speicherfrist bemisst sich danach:

1) Wie lange die Daten zur Erfüllung der Hochschulaufgaben benötigt werden (frühestmögliche Löschung)
2) Ob es darüber hinaus rechtliche Vorgaben zur Speicherung/Aufbewahrung gibt

Für die TUD gilt § 18 Abs. 1 S. 2 SächsHSPersDatVO:

„Das Nähere, auch die Fristen, nach denen eine Löschung erfolgt, regeln die Hochschulen durch Ordnung.“

Konkrete Vorgaben innerhalb der TUD (insb. Rundschreiben UA 01/2018 + neue Ordnung)

- Studierenden- und Prüfungsakten* (2-30 Jahre nach Exmatrikulation; Restakte 5 Jahre)
- Promotions- und Habilitationsakten* (5-30 Jahre nach Abschluss der Promotions- und Habilitationsverfahren)
- Personaldaten* (nach 4.1 VwV Personalakten und G I.1. VwV PersAktenB i.d.R. 5 Jahre nach Beendigung des Arbeitsverhältnisses)
- Daten aus Stellenbewerbungen (gem. § 11 Absatz 4 SächsDSDG unverzüglich nach Abschluss des Auswahlverfahrens; max. 4 Monate)

* Sind vor der Löschung/Vernichtung dem Uniarchiv anzubieten

Konkrete Vorgaben innerhalb der TUD (insb. Rundschreiben UA 01/2018 + neue Ordnung)

- Forschungsdaten, § 12 Absatz 2 SächsDSDG:

„… soweit es der Forschungszweck erlaubt, [sind] **die Merkmale**, mit deren Hilfe ein Personenbezug hergestellt werden kann, getrennt zu speichern; **die Merkmale** sind zu löschen, sobald der Forschungszweck dies zulässt“

- Daten, die zur Beilegung einer Rechtsstreitigkeit erforderlich sind

➢ vollständig und dauerhaft zu archivieren

Umsetzung der Löschung

Art. 24 Abs. 1 DSGVO:

„Der Verantwortliche setzt unter Berücksichtigung […] der Zwecke der Verarbeitung […] und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische […] Maßnahmen um."

- physische Zerstörung bzw. fachmännische Entsorgung
- Überschreiben der Speicherplätze
- Löschungen von Verknüpfungen oder Codierungen
- Anonymisierung (s. oben)
- Recht auf Vergessenwerden (Auslistung bei Suchmaschinen)

Umsetzung der Löschung / Backup und Snapshots

- gesetzliche Verpflichtung zur Sicherheit der Verarbeitung (Art. 32 DSGVO / Verfügbarkeit und Wiederherstellbarkeit)
- Planung von Backups (file-bezogen)
- Problem: Snapshots nicht file-bezogen
- Abwägung Löschung vs. Sicherheit der Verarbeitung
- Milderung durch zusätzliche Maßnahmen bei der Wiederherstellung

Löschkonzept nach DIN 66398

- Bestimmung der Datenarten (z.B. nach Zweck)
- Zusammenfassung der Datenarten in Löschklassen
- Definition einer Löschregel pro Löschklasse
- Definition von konkreten Umsetzungsregeln
- Definition der jeweils Verantwortlichen für die Umsetzung
- Dokumentation der ergriffenen und zu ergreifenden Schritte und Pflege der Dokumentation

GSM – praktische Hinweise

Erläuterung Schwachstellenmeldung

Meldung von Centreon per E-Mail

***** Centreon Notification *****

Type: PROBLEM
Service: GSM
Host: XXX
Address: XXX
State: WARNING
Date/Time: 17-05-2021/01:26:23
Info: GMP WARNING: 8 vulnerabilities found - High: 0 Medium: 6 Low: 2
Details: For security reasons, no details are transmitted. Please use the centreon-link below and log in with your ZIH credentials. Note the NVT-Codes for each vulnerability within the extended status information.
Afterwards, connect to "https://secinfo.cert.tu-dresden.de/nvts" as guest(!) and look up the NVT-Codes with the filter field.
As soon as you fixed the mentioned vulnerabilities, use the GSM-Rescan-Button (available for Enterprise-VMs only): "https://selfservice.zih.tu-dresden.de/l/index.php/cloud_dienste/ep_vms"

Link: https://centreon.zih.tu-dresden.de/main.php?p=XXXXXXXXXXXX

→ Direktlink führt zur Centreon-Webseite mit weiteren Informationen

Erläuterung Schwachstellenmeldung

Detaillierte Übersicht der gefundenen Schwachstellen

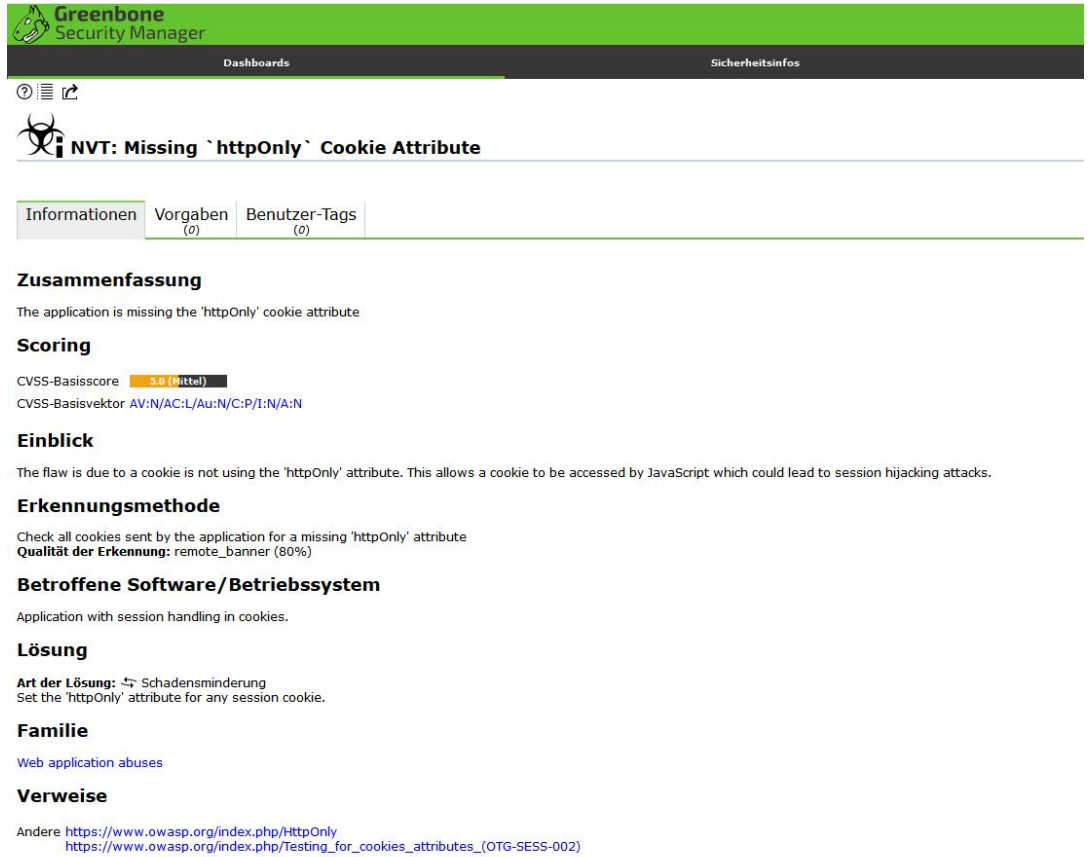
- NVT OID zur Spezifizierung der Schwachstelle
- Ausführliche Informationen zur Schwachstelle sowie zur Behebung unter https://secinfo.cert.tu-dresden.de
- Direktlink ist in Centreon Meldung enthalten
- Alternative: Manuelle Suche der NVT OID im Secinfo-Portal

Erläuterung Schwachstellenmeldung

Startseite Secinfo Portal

- Anmeldung als Gast
- ZIH-Login Daten funktionieren nicht

Erläuterung Schwachstellenmeldung



Greenbone Security Manager

Dashboards | Sicherheitsinfos

NVT: Missing `httpOnly` Cookie Attribute

Informationen | Vorgaben (0) | Benutzer-Tags (0)

Zusammenfassung

The application is missing the 'httpOnly' cookie attribute

Scoring

CVSS-Basisscore 5.0 (Mittel)

CVSS-Basisvektor AV:N/AC:L/Au:N/C:P/I:N/A:N

Einblick

The flaw is due to a cookie is not using the 'httpOnly' attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Erkennungsmethode

Check all cookies sent by the application for a missing 'httpOnly' attribute
Qualität der Erkennung: remote_banner (80%)

Betroffene Software/Betriebssystem

Application with session handling in cookies.

Lösung

Art der Lösung: Schadensminderung
Set the 'httpOnly' attribute for any session cookie.

Familie

Web application abuses

Verweise

Andere https://www.owasp.org/index.php/HttpOnly
https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002)

- Detail-Übersicht der Schwachstelle
- Schweregrad
- Erläuterung & Erkennungsmethode
- Lösungsvorschlag von Greenbone

Manueller Rescan eines Server

- Möglichkeit über das Self-Service-Portal einen manuellen Rescan einer VM auszulösen, z.B. nach Behebung von Sicherheitslücken
- Reguläre Scans laufen nur einmal wöchentlich, somit lange Wartezeit bis aktuelles Ergebnis vorliegt
- Self-Service-Portal → Cloud-Dienste → Enterprise Cloud → VM Management

- Löst einen Rescan im GSM aus → Ergebnis im Centreon

Überprüfung Scan-Status

Statusabfrage des letzten GSM Scans

	NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091) NVT Link: https://secinfo.dez.tu-dresden.de/nvt/1.3.6.1.4.1.25623.1.0.80091 SEVERITY: Low (2.6) PORT: general/tcp DESCR: It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 3391440970 Packet 2: 3391442549
	SCAN_END: 2021-05-16T19:13:26Z
Performance Data	
Current Attempt	1 / 1
State Type	HARD
Last Check Type	Active
Last Check	2021/05/17 - 09:56:25
Next Scheduled Active Check	2021/05/17 - 10:26:25
Latency	0.14 seconds
Check Duration	0.097517 seconds
Last State Change	2021/03/01 - 00:09:44
Current State Duration	2M 2w 2d 11h 55m 10s

- SCAN_END relevant wann letzter GSM Check durchgeführt wurde
- Last Check irrelevant (nur Datenabfrage von Centreon und GSM)

GSM-Override für Schwachstellen

- Ausnahmeregelung für Schwachstellen welche kurz-/mittelfristig nicht behoben werden können
- z.B.: TLS-Policy
- Anfrage mit Begründung/Erläuterung zur Schwachstelle an: cert@tu-dresden.de
- Schwachstelle wird nach Prüfung der Anfrage für einen festgelegten Zeitraum herabgestuft

ENDE