IT-Security Awareness Penetration Testing

Erläuterung der Problemstellung, die mit der Idee gelöst werden soll:

Wichtiges Instrument eines systematischen Risikomanagements ist die Bewertung von Aufwand und Nutzen Risikolimitierender Sicherheitsmaßnahmen. Zur Quantifizierung der IT-Sicherheit in Unternehmen werden üblicherweise Penetration-Tests und Audits der IT-Systeme durchgeführt. Diese lassen den Menschen als wesentlichen Teil der IT-Sicherheitsbewertung außer Acht. Ein gesamtheitlicher und systemischer Ansatz muss den Nutzer und seinen Interaktionsraum miteinbeziehen. Die Problemstellung zeigt sich in diesem Zusammenhang dual.

Zur Prävention von IT-Sicherheitsvorfällen werden die Nutzer ganz unterschiedlichen Interventionen ausgesetzt (E-Learning-Plattformen, Videotrainings, Schulungen, Marketingkampagnen mit Postern und Flyern und viele mehr). Die Wirkung dieser Maßnahmen auf die IT-Sicherheit des Unternehmens wird jedoch nur selten bewertet, Welche Maßnahme ist die richtige? Kann eine Maßnahme das Verhalten der Nutzer so beeinflussen, dass die Nutzer Sicherheitsvorfälle vermeiden, diese aber immer noch bei entsprechenden Stellen (zum Beispiel einem IT-Helpdesk) anzeigen ohne die entsprechende Stelle zu überlasten?

Neben den Maßnahmen sollten Charakteristika des Umfeldes vermessen werden. Insbesondere sind hier Faktoren von Interesse die sich auf den Stress des Nutzers auswirken können. So können sich bestimmte Zeiten und Ereignisse wie ein Firmenzusammenschluss, der Jahresabschluss oder die Integration neuer IT-Systeme wie Windows 10 auf die IT-Security-Awareness auswirken. Aber auch die Lage des Arbeitsplatzes, der Geräuschpegel oder Kundenkontakt können eine Rolle spielen. Auch die Arbeitskultur in einer Abteilung ist von Interesse, wie gestattete Reaktionszeiten auf Kommunikationsanfragen und die Häufigkeit von Unterbrechungen. Wirkt sich eine bring-you-own-device-Strategie positiv auf die IT-Security-Awareness aus, weil der Nutzer mit dem Interaktionsrahmen vertrauter ist?

Zur Beantwortung dieser Fragen fehlt es aktuell an einem Werkzeug, das einen belastbaren Einblick in den sicherheitsrelevanten Entscheidungsprozess der Nutzer beim Umgang mit IT erlaubt. Für die heutige Gesellschaft ist es unabdingbar in den Verbund aus Mensch und IT zu investieren um Wissen schaffen zu können, dass die Möglichkeit eröffnet diesen nachhaltig zu verbessern.

Beschreibung der Idee und wie sie das Problem lösen soll:

Die Grundidee ist, das Prinzip vom technischen Sicherheitstest auf den Nutzer zu übertragen. Bei technischen Sicherheitstests wird ein Angriff auf die IT-Infrastruktur simuliert, Daten über die Infrastruktur während der Simulation gesammelt und im Anschluss ausgewertet. Analog zu diesem Prinzip wird ein Nutzer in seiner gewohnten Arbeitsumgebung mit ungewohnten Reizen konfrontiert und die von ihm ergriffenen Handlungsoptionen werden erfasst. Diese können dann bezüglich ihrer Repräsentation von IT-Security-Awareness hin, interpretiert werden. Eine derartige Auswertung kann nach verschiedenen Aspekten wie Arbeitsplatzbeschaffenheit oder Abteilungszugehörigkeit aufgeschlüsselt werden und ermöglicht so einen Einblick in die IT-Security-Awareness der Mitarbeiter und gibt Hinweise auf ihre Einflussfaktoren. Sind

diese identifiziert so können die Einflussfaktoren gezielt adressiert werden. Dabei sollte nicht der Nutzer im Vordergrund stehen, sondern die technische Umgebung in der dieser agiert.

Für die korrekte Interpretation der durch den Probanden ergriffenen Handlungsoption ist das Wissen um die entscheidungsrelevanten Elemente der Situation in der die Entscheidung getroffen wurde, unabdingbar. Da eine Situation, die ein Nutzer in seinem Alltag durchlebt nicht vollständig zu erfassen, die Kontrolle über die entscheidungsrelevanten Elemente der Situation aber unabdingbar ist, gilt es diese Elemente kontrolliert in die Situation einzubringen. Der Nutzer verfolgt mit dem Haupthandlungsstrang ein Ziel. Dabei durchläuft er eine Reihe aufeinander folgender und ineinander übergehender Situationen. Diese sind durch verschiedene Elemente charakterisiert. Einige davon haben einen Sicherheitsbezug. Dieser kann sich auf natürliche Weise ergeben, etwa eine Passwortabfrage beim Zugriff auf eine geschützte E-Mail, oder aber künstlich in die Situation eingebracht werden, z.B. eine Passwort-Abfrage auf einer sogenannten „Landing-Page“. Wird ein Element derart künstlich eingebracht, ist es ein Artefakt.

Selbst wenn Artefakte kontrolliert in eine Situation eingebracht wurden und die vom Nutzer ergriffene Handlungsoption erfasst ist, lässt sich kein direkter Rückschluss auf die IT-Security-Awareness des Nutzers ziehen. Der Einfluss anderer entscheidungsrelevanten Faktoren ist zu groß und es gilt diesen Einfluss beherrschbar zu machen. Zur Erfassung der entscheidungsbeeinflussenden Charaktereigenschaften lässt sich ein Fragebogen entwerfen, der diese erfassbar macht. Die ermittelten Charaktereigenschaften müssen dann mit der Bewertung der Handlung korreliert werden. Zur Beherrschung situativer Einflüsse, ohne die Möglichkeit, die Situation selbst zu kontrollieren, steht die Mehrfachausführung, angelehnt an die Effektgrößeneinschätzung einer Meta-Analyse, zur Verfügung. Dieses Vorgehen hat zur Folge, dass situative Einflüsse und die Qualitätsmerkmale der Artefakte (wie deren Sichtbarkeit) nicht signifikant in das Ergebnis einfließen.

An dieser Stelle setzt das ITS.APT-Framework (ITS.APT: „IT-Security Awareness Penetration Testing“) an. Es automatisiert die zur IT-Security-Awareness-Messung benötigten Vorgänge. Es ist in der Lage, auf Basis von Ablaufplanungen, Artefakte in den Wahrnehmungsbereich der Nutzer einzubringen und ergriffene Handlungsoptionen datenschutzkonform aufzuzeichnen. Außerdem werden weitere rechtliche Anforderungen, etwa aus arbeitsrechtlicher Sicht, umgesetzt.

Auswertungen werden anhand der erfassten, durch den Teilnehmer ergriffenen Handlungsoptionen bestimmt. Um diese mit Hilfe einer Skalierung vergleichbar zu machen, werden die einzelnen Handlungsoptionen mit einem Punktewert belegt. Dieser entsteht zunächst durch die Einschätzung eines Experten, wird aber im Laufe der Zeit durch einen kontinuierlichen Messwerte-Feedback- Prozess angepasst. Die Tatsache, dass die ergriffene Handlungsoption sowie ihre Bewertung aufgezeichnet werden, erlaubt die Vergleichbarkeit der Ergebnisse auch über größere Zeiträume hinweg. So lässt sich die Weiterentwicklung der IT-Security-Awareness von Nutzern auch in Längsschnittstudien untersuchen. Dies erlaubt die Bewertung von IT-Security-Awareness-Kampagnen und -Schulungen.

Das Framework unterstützt per Design ausschließlich pseudonymisierte oder anonymisierte Ergebnisberichte. Idealerweise werden so ausschließlich einer Teilnehmergruppe oder einem Artefakt zugeordnete Berichte genutzt. Sollen jedoch gezielt Teilnehmer geschult werden, so

müssen die Ergebnisse mit der Identität der Teilnehmer korrelierbar sein. In diesem Fall ist ein pseudonymisierter Bericht zu nutzen. Das Pseudonym jedes Teilnehmers ist dann in der Datei mit der Auflistung der Teilnehmergruppe kodiert. Die Auflösung des Pseudonyms ist so ausschließlich dem Besitzer der Datei möglich. Wird die Datei nach der Testdurchführung gelöscht, so wird den Pseudonymen die Möglichkeit der Aufdeckbarkeit entzogen (sofern keine weitere Kopie existiert). Dies gewährleistet den maximalen Schutz der Persönlichkeitsrechte.

Mit dem ITS.APT-Framework werden systematisiert in Computernetzwerken von Unternehmen, die individuelle sowie die kollektive IT-Security-Awareness der Mitarbeiter ermittelt. Dabei kommen sichere Verfahren zur Pseudonymisierung und Anonymisierung zum Einsatz, sodass Persönlichkeitsrechte, Arbeitnehmerrechte als auch Datenschutzrechte der Probanden gewahrt bleiben. Insbesondere wird verhindert, dass Rückschlüsse auf persönliche Lebensumstände möglich sind. Damit werden die Grundvoraussetzungen erfüllt, um die in jedem Fall notwendige Zustimmung der Personalvertretung und des Datenschutzes für die Durchführung von Mitarbeiterbeobachtungen zu erzielen.

Um diese Idee zu verwirklichen muss ein technisches Rahmenwerk geschaffen werden, das die Ausbringung beliebiger Reize (z.B. Phishing-E-Mails, Pop-Ups, Websitedefacings) erlaubt und die Aufzeichnung der Nutzeraktionen in Reaktion auf diese Reize ermöglicht. Dies ist uns im BMBF-geförderten Projekt ITS.APT gelungen. Im Rahmen des Projekts wurde auch der rechtliche Rahmen evaluiert, in dem der Einsatz dieses Werkzeugs möglich ist. Auch Referenzdokumente, die für einen rechtskonformen Einsatz nötig sind, wurden im Rahmen dieses Projekts erarbeitet. So liegen durch die im Rahmen des Projekts ITS.APT abgeschlossenen Arbeiten bereits Muster für Betriebs- und Dienstvereinbarungen vor. Eine derartige Vereinbarung ist ein Instrument der betrieblichen Mitbestimmung und enthält Bestimmungen mit unmittelbarer Auswirkung auf das Arbeitsverhältnis. Gleichzeitig dient die Vereinbarung auch als datenschutzrechtliche Erlaubnisnorm. Darüber hinaus fordert der Datenschutz einen Eintrag in das Verfahrensverzeichnis. Auch für dieses steht ein Mustereintrag nach §7 Abs. 3 des Landesdatenschutzgesetz Schleswig-Holstein bereit. Dieser bildet wiederum die Grundlage für eine Datenschutz-Folgenabschätzung gemäß Artikel 35 Datenschutz-Grundverordnung.

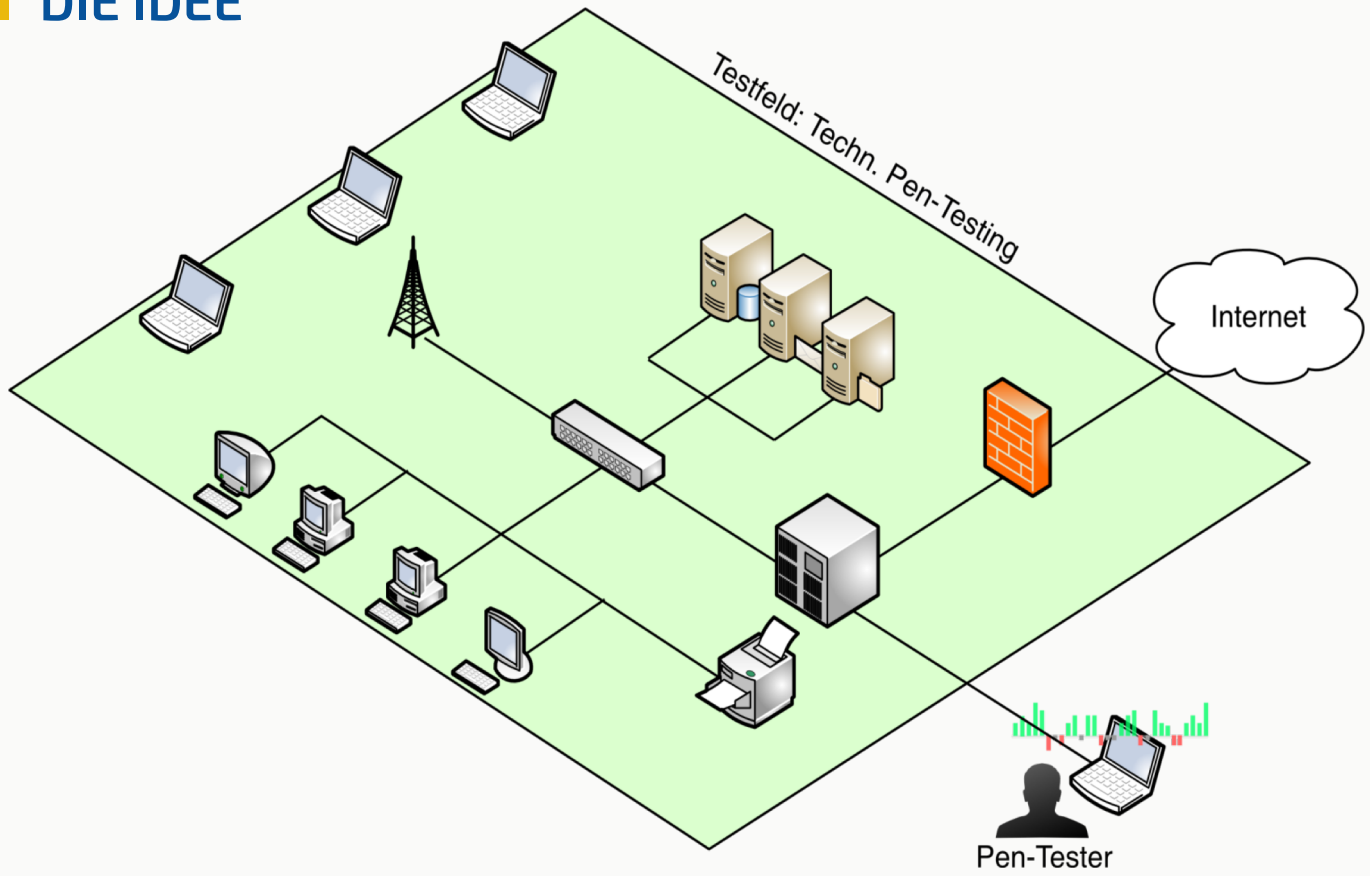
UNIVERSITÄT BONN

Prof. Dr. Michael Meier
itsapt@uni-bonn.de
https://itsec.cs.uni-bonn.de/itsapt

„IT-SECURITY AWARENESS PENETRATION TESTING“ IN 7 MINUTEN

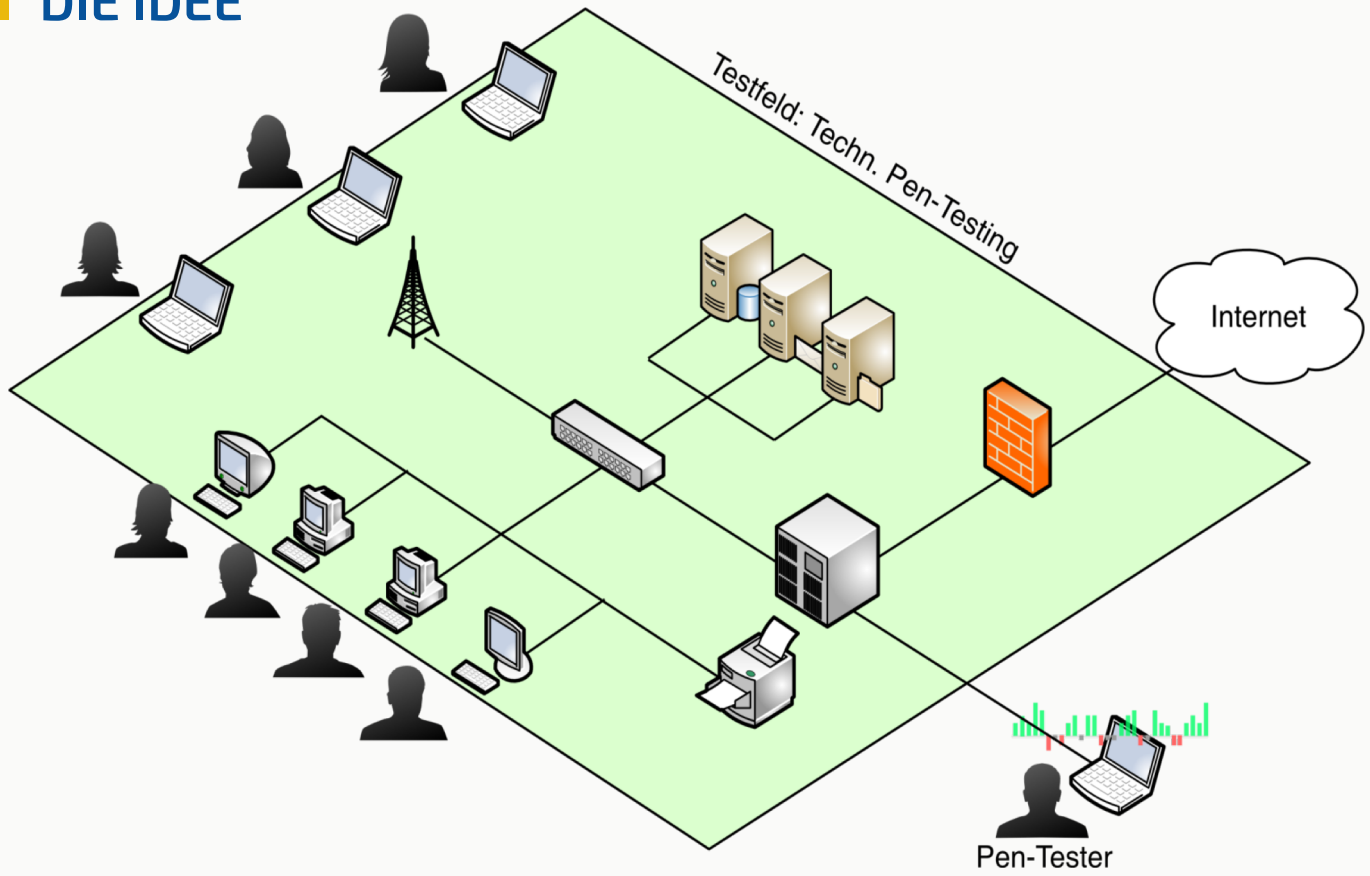
UNIVERSITÄT BONN

DIE IDEE



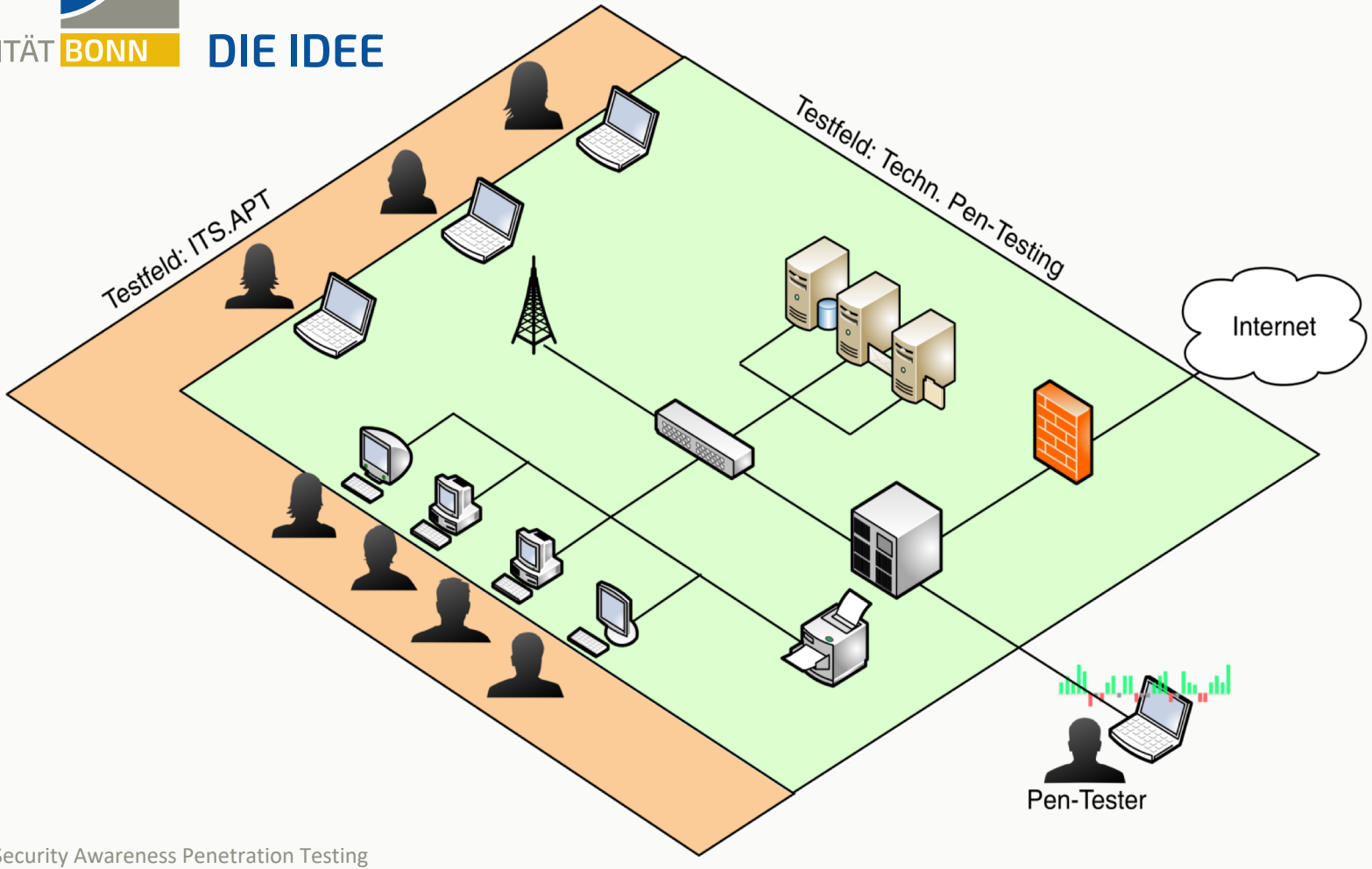
UNIVERSITÄT BONN

DIE IDEE



UNIVERSITÄT BONN

DIE IDEE



UNIVERSITÄT BONN

DAS NUTZERVERHALTEN BEEINFLUSST ZWEI ASPEKTE

Prävention **Detektion**

UNIVERSITÄT BONN

STAND DER TECHNIK

UNIVERSITÄT BONN

PHISHINGTESTS

UNIVERSITÄT BONN

PHISHINGTESTS

UNIVERSITÄT BONN

PHISHINGTESTS

UNIVERSITÄT BONN

PHISHINGTESTS

UNIVERSITÄT BONN

PHISHINGTESTS

UNIVERSITÄT BONN

PHISHINGTESTS

UNIVERSITÄT BONN

PHISHINGTESTS

STEIGERUNG DES SICHERHEITSBEWUSSTSEIN

SCHULUNGEN

STEIGERUNG DES SICHERHEITSBEWUSSTSEIN

SCHULUNGEN

UNIVERSITÄT BONN

IT-SECURITY AWARENESS PENETRATION TESTING ENVIRONMENT

PROBLEME

- Phishing-E-Mails sind nur *ein* mögliches Artefakt
- Detektion wird nicht gemessen!
  - Prävention ist nicht perfekt
  - Detektion ist wichtig!

PROBLEME

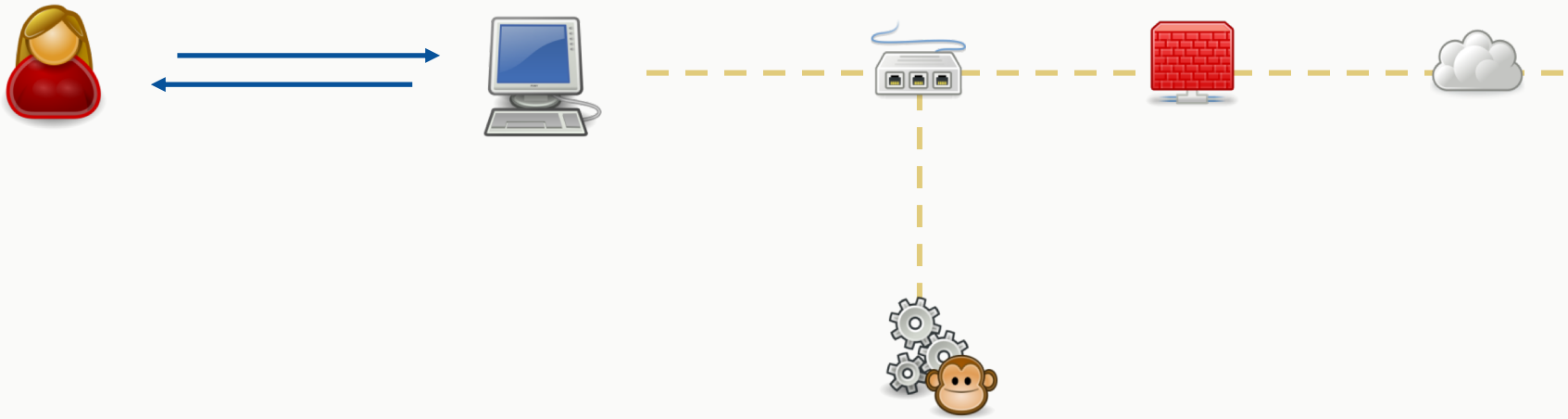
- Phishing-E-Mails sind nur *ein* mögliches Artefakt
- Detektion wird nicht gemessen!
  - Prävention ist nicht perfekt
  - Detektion ist wichtig!

UNIVERSITÄT BONN

DAS WERKZEUG

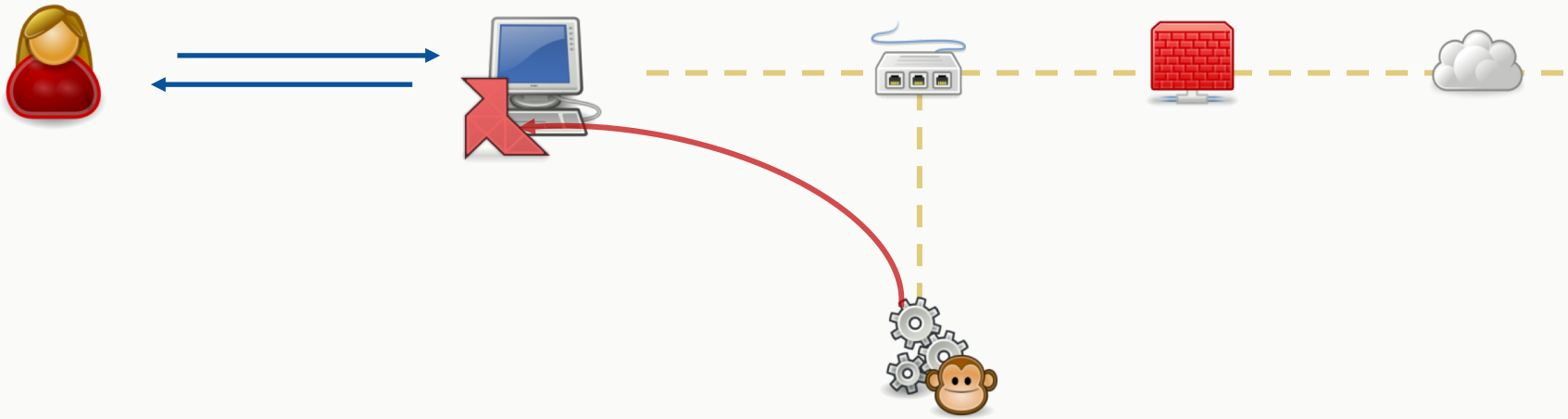
UNIVERSITÄT BONN

DAS WERKZEUG



UNIVERSITÄT BONN

DAS WERKZEUG

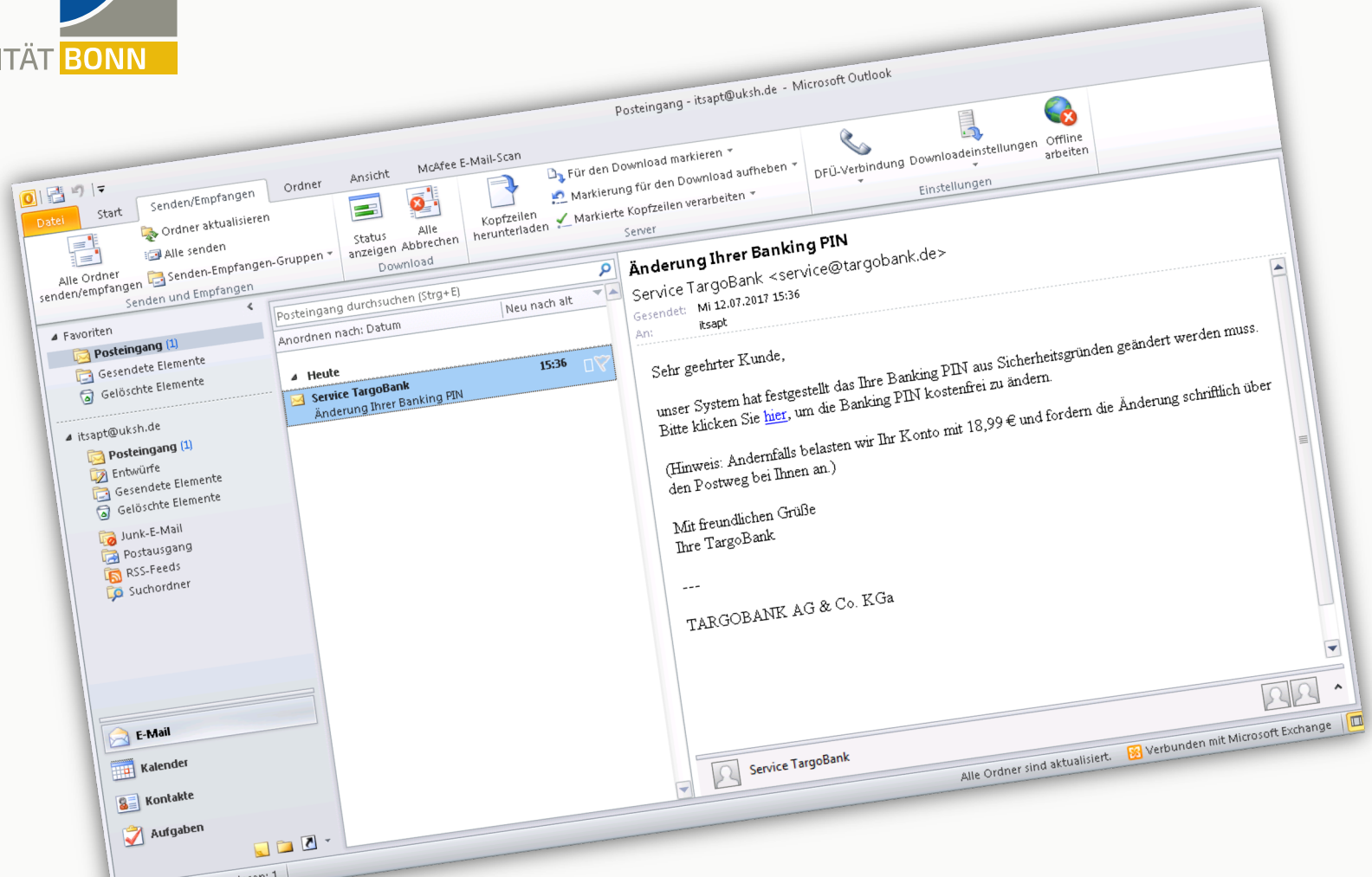


UNIVERSITÄT BONN

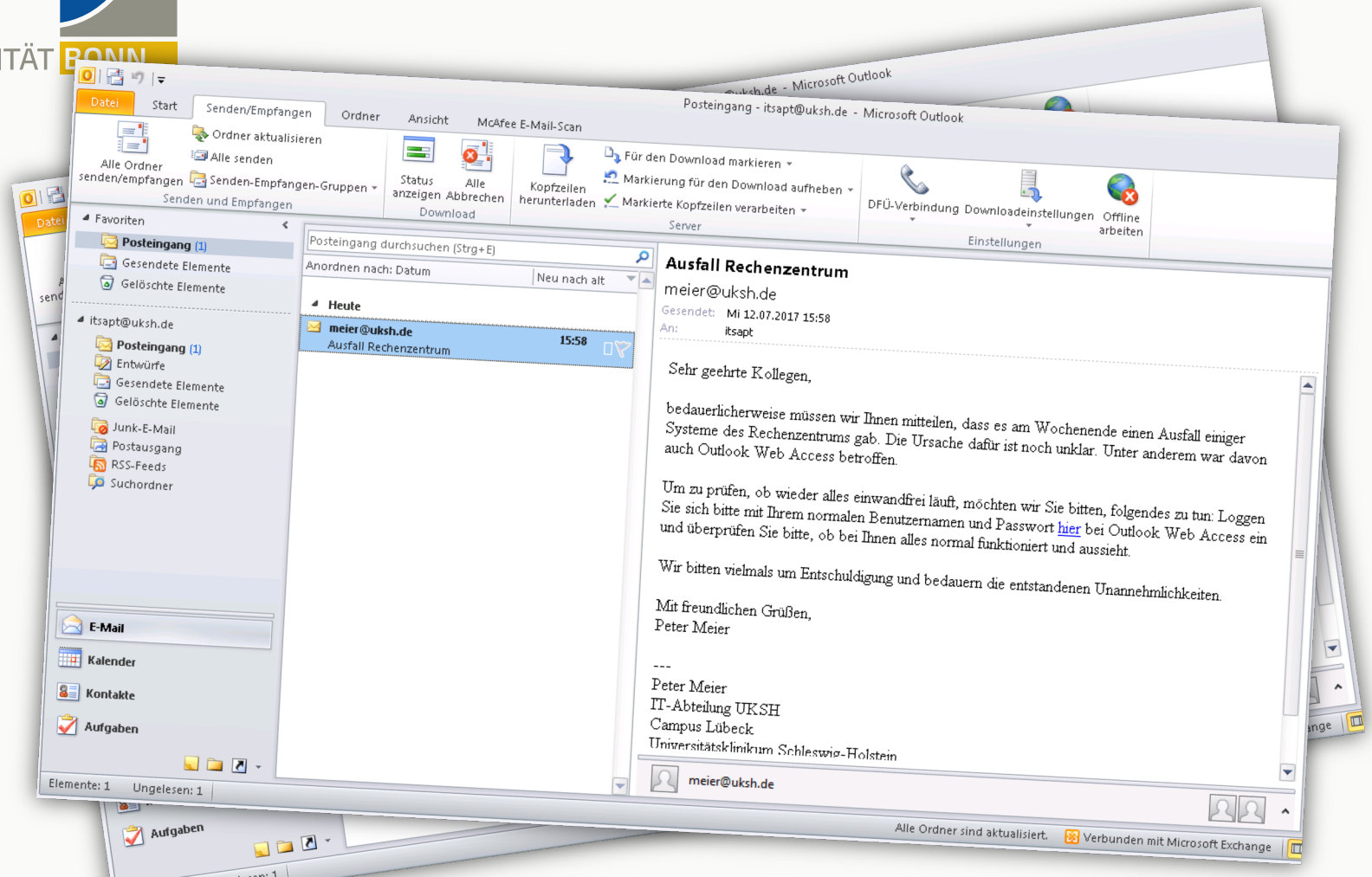
ATEFAKTE

?

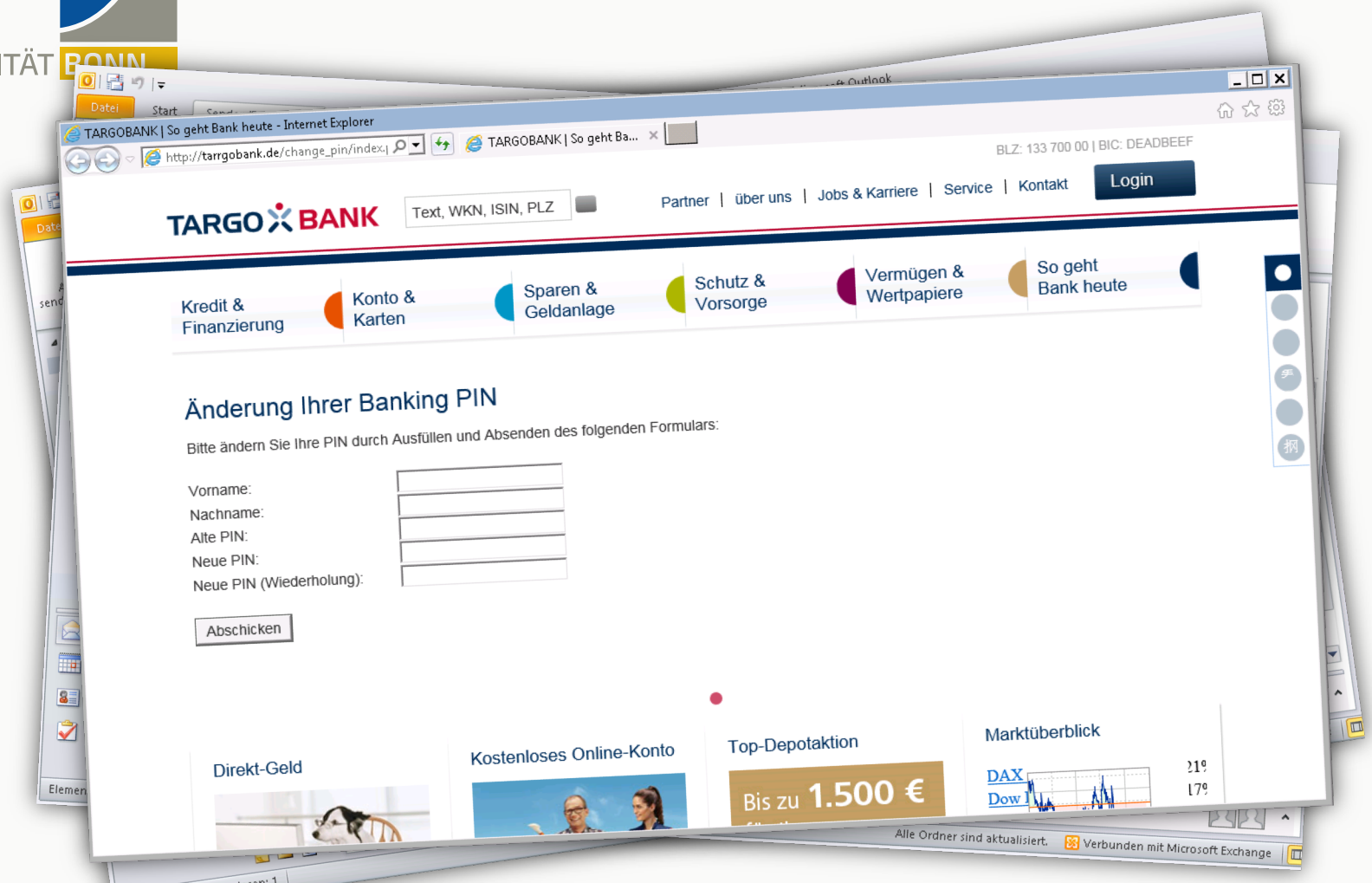
UNIVERSITÄT BONN



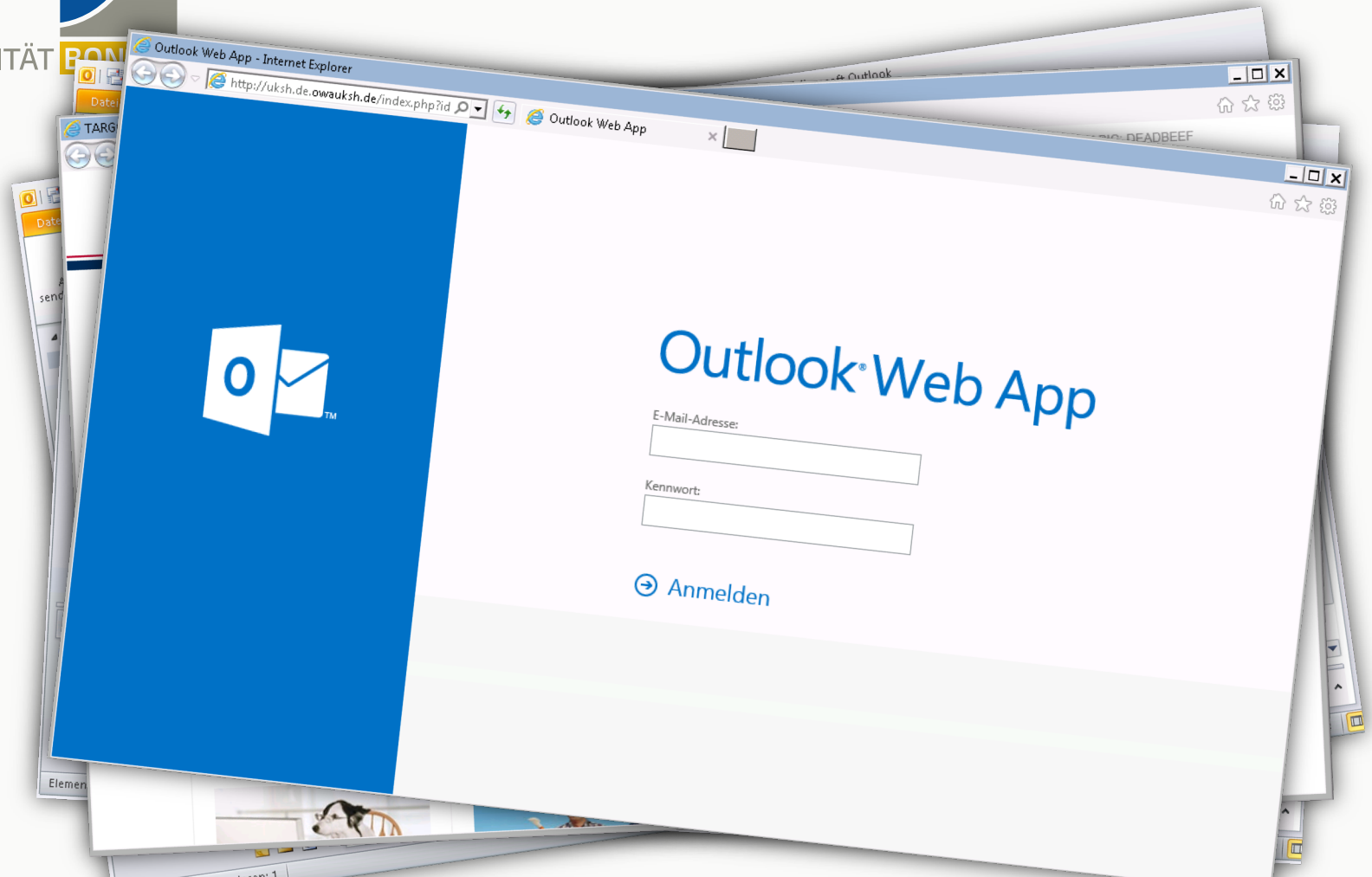
UNIVERSITÄT BONN



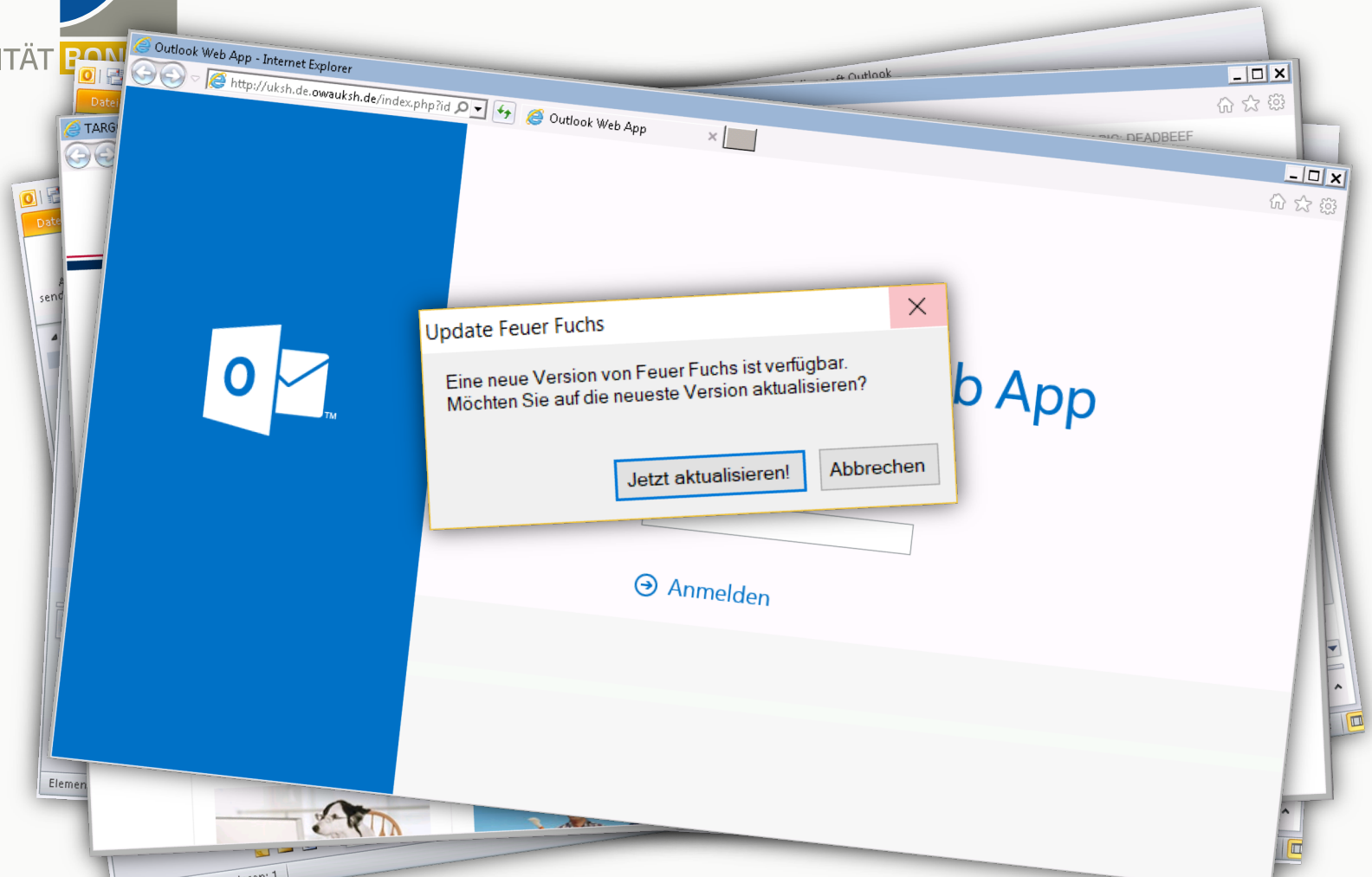
UNIVERSITÄT BONN



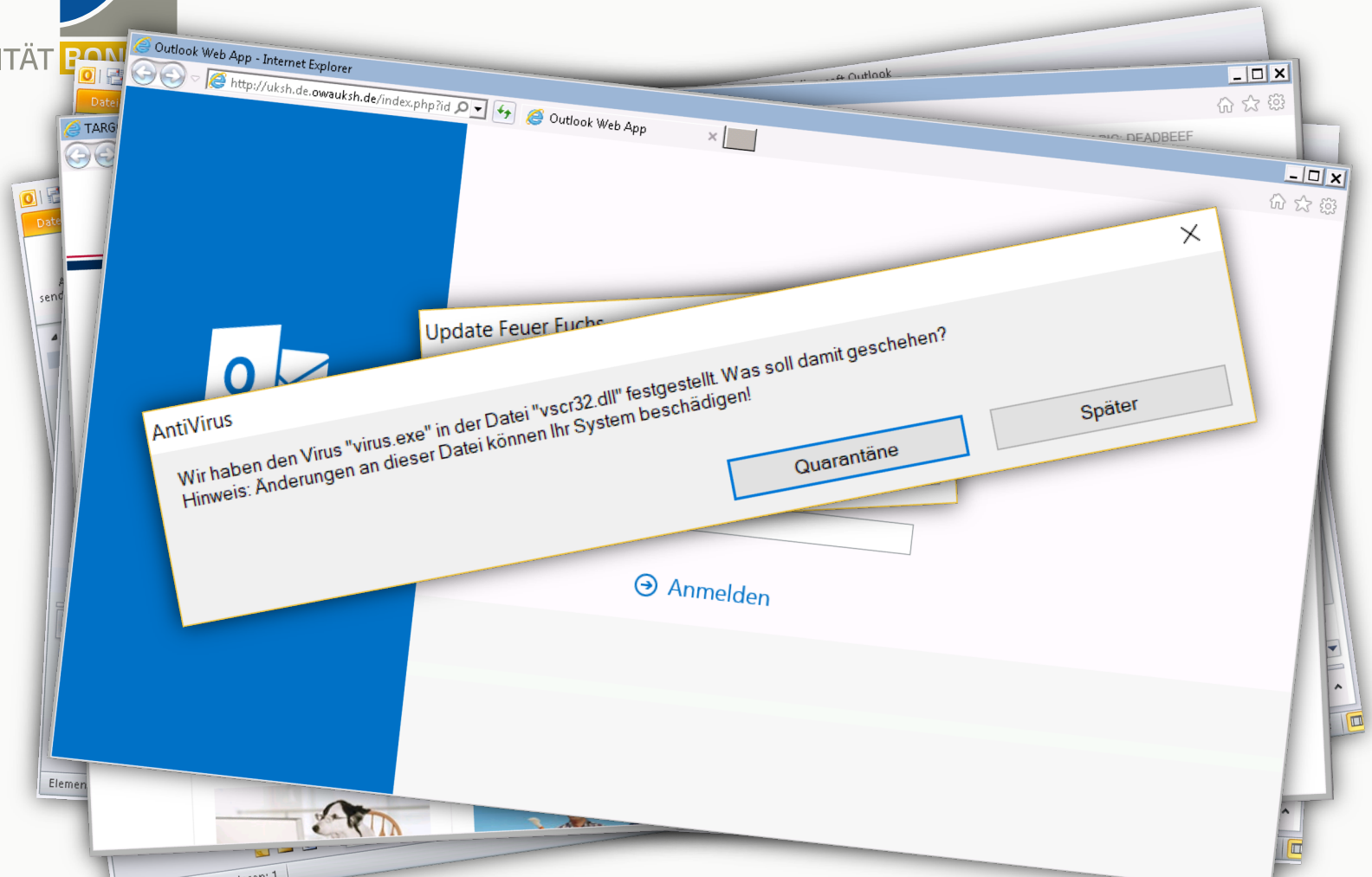
UNIVERSITÄT BONN



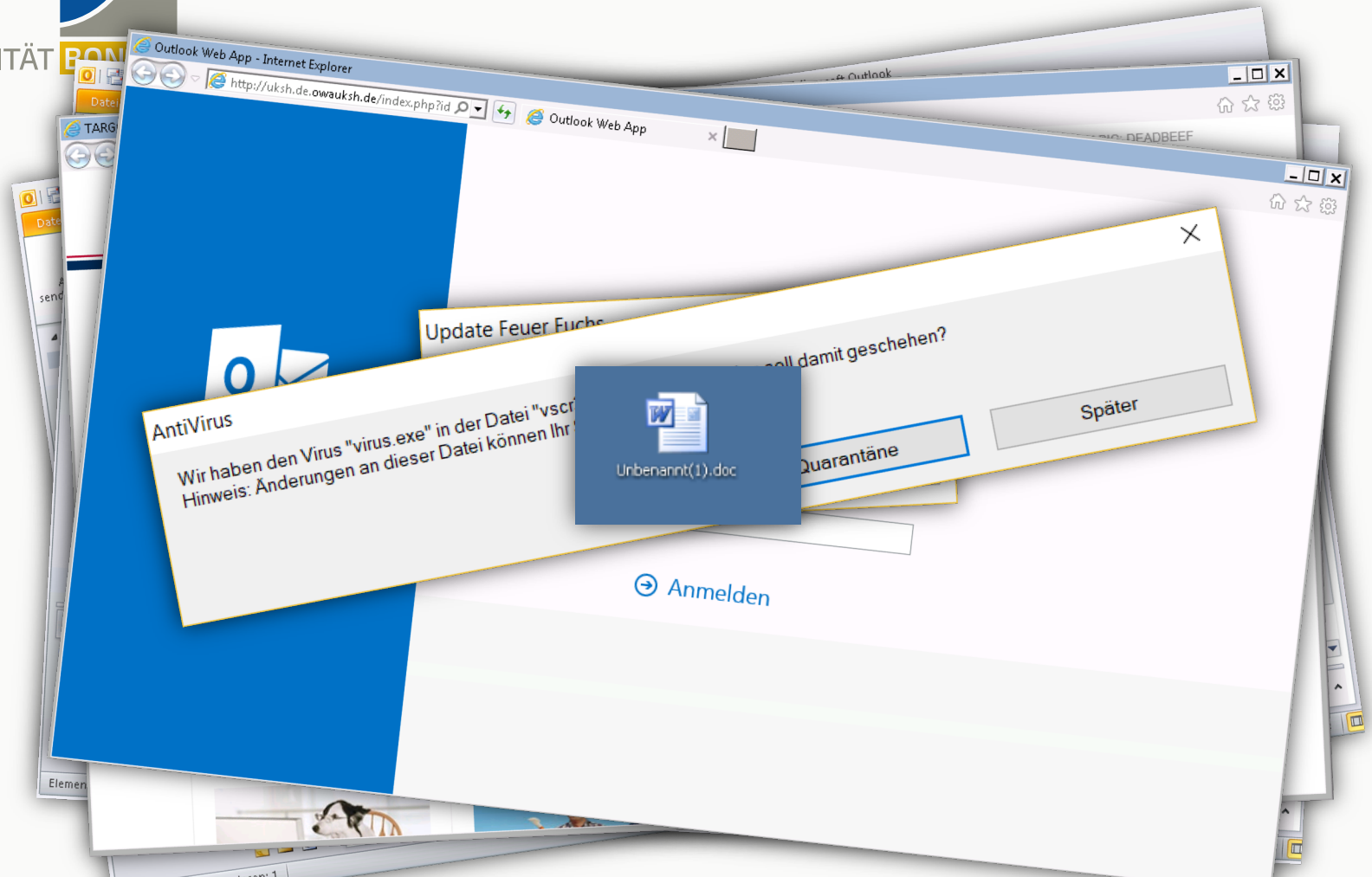
UNIVERSITÄT BONN



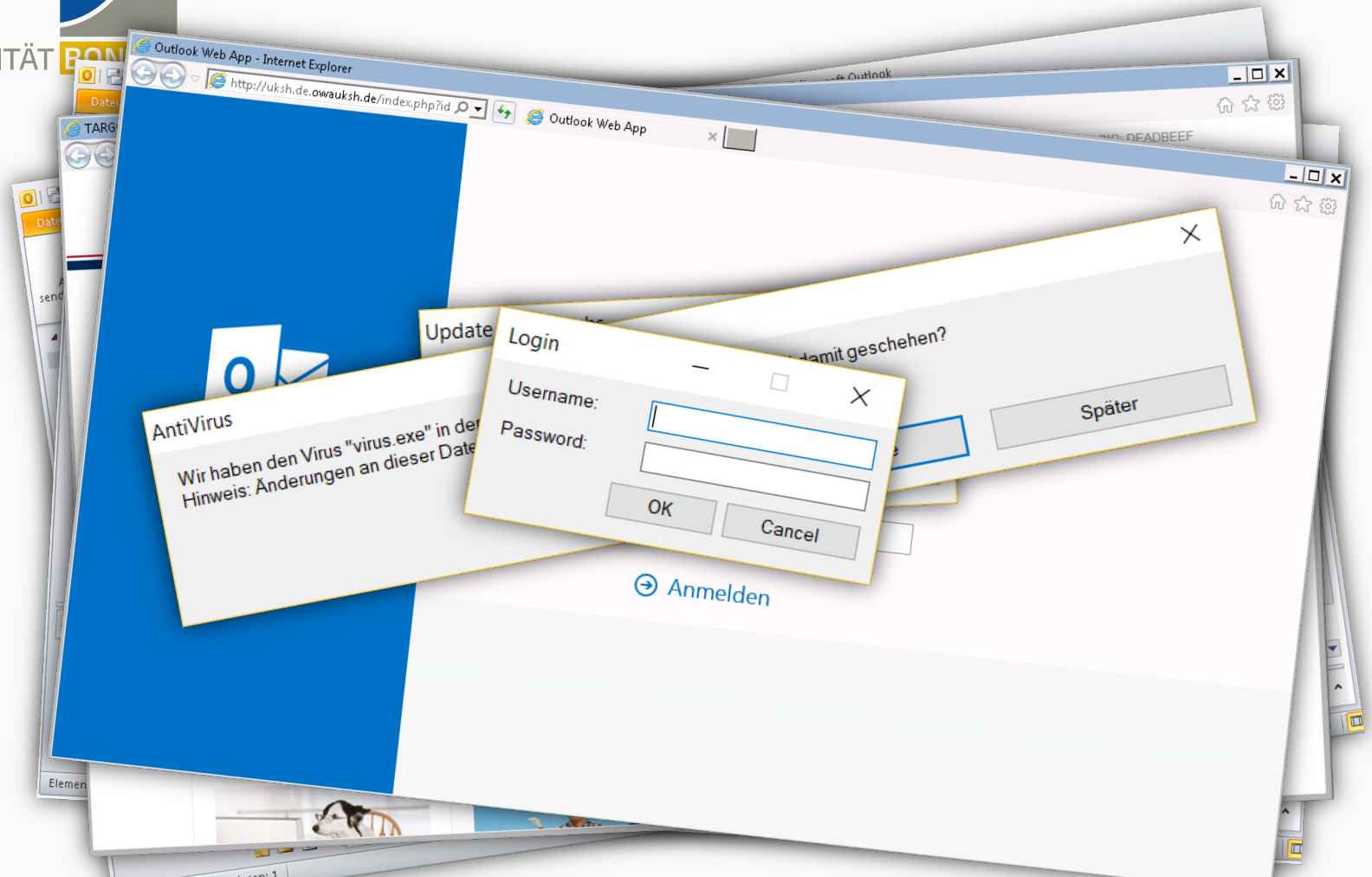
UNIVERSITÄT BONN



UNIVERSITÄT BONN



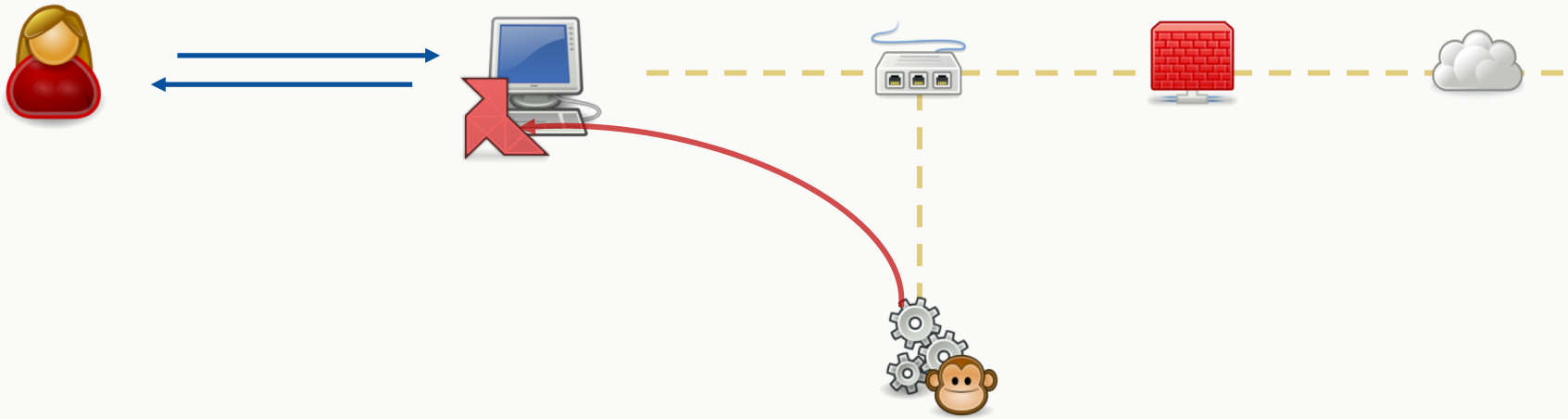
UNIVERSITÄT BONN



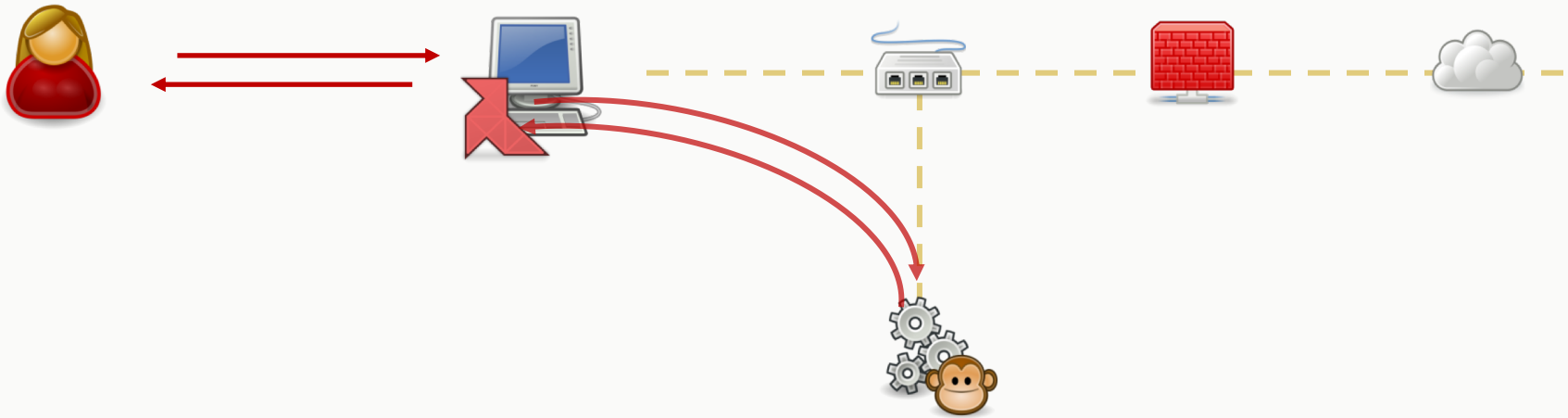
PROBELME

- Phishing-E-Mails sind nur *ein* mögliches Artefakt
- Detektion wird nicht gemessen!
  - Prävention ist nicht perfekt
  - Detektion ist wichtig!

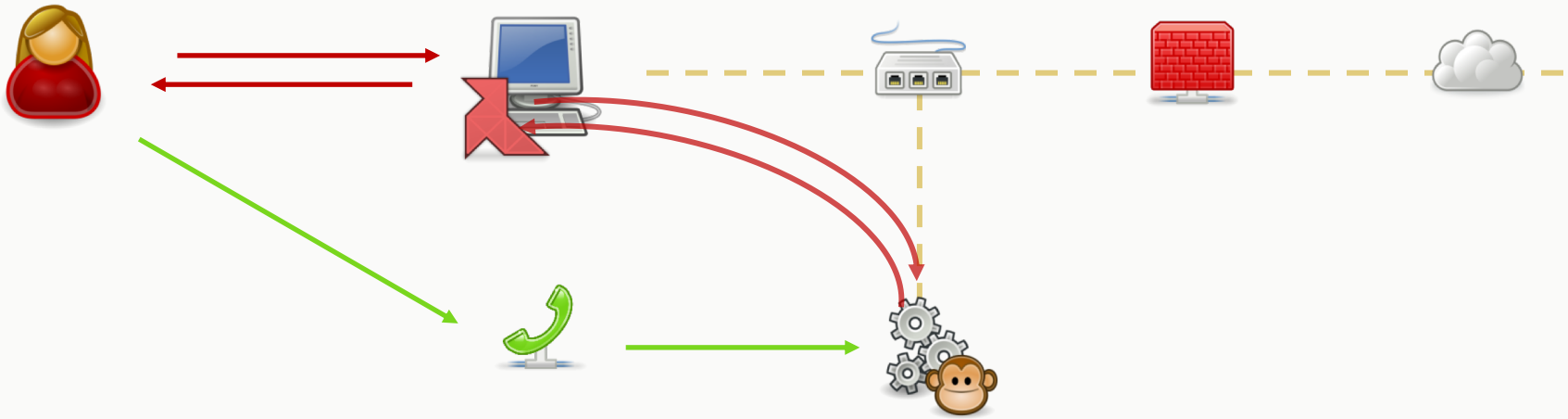
DAS WERKZEUG



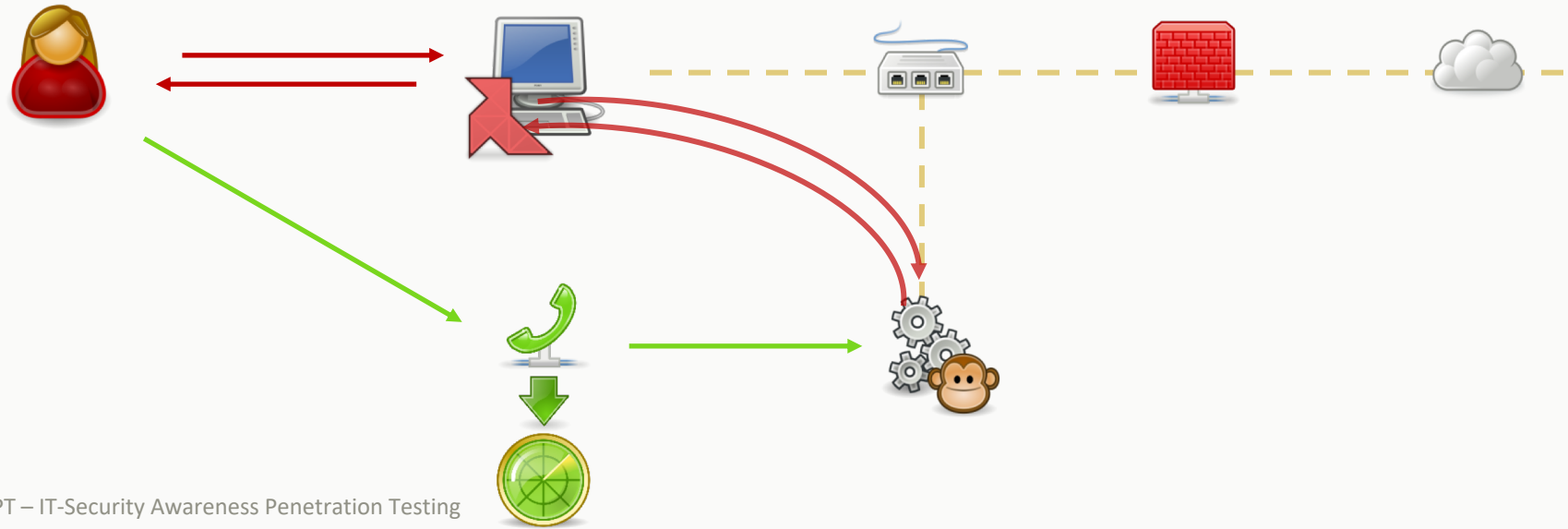
DAS WERKZEUG



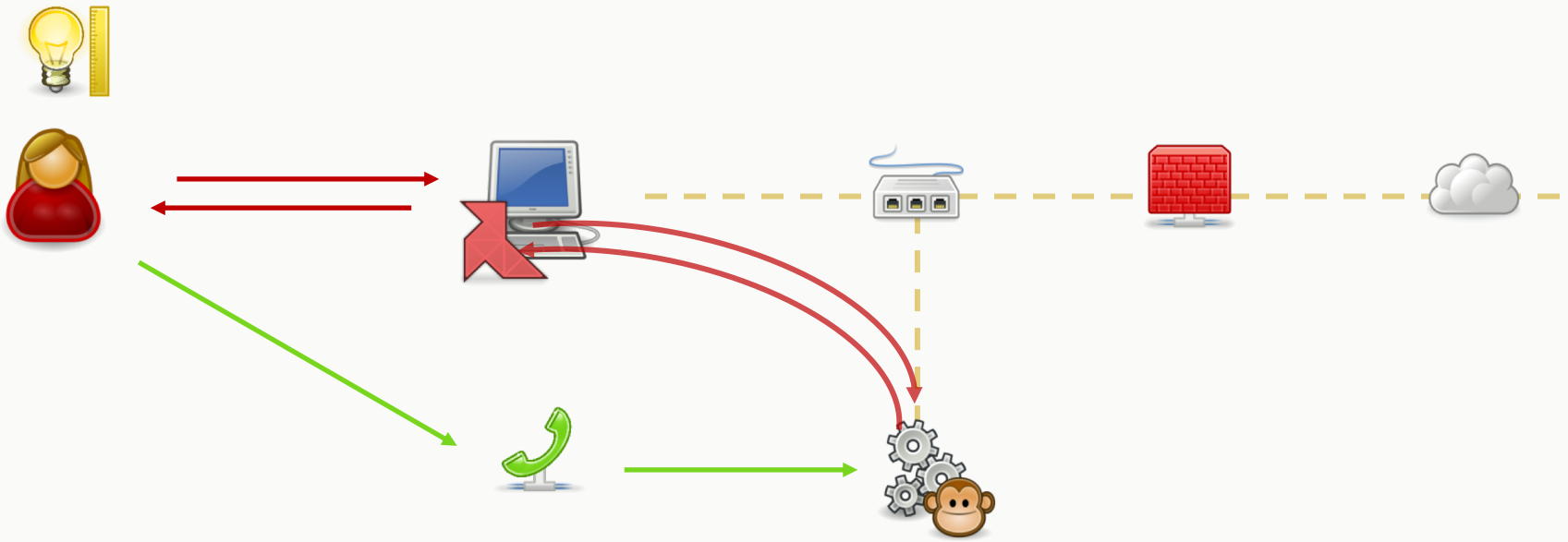
DAS WERKZEUG



DAS WERKZEUG



DAS WERKZEUG



UNIVERSITÄT BONN

MESSERFAHRUNG

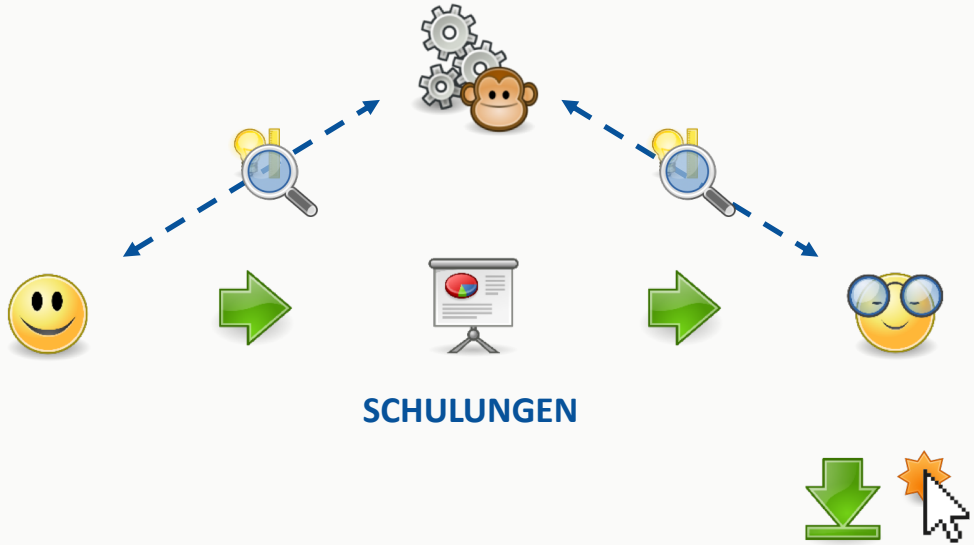
- **Eine Studie** mit **zwei Messphasen**:
  Testen, Schulen, Testen
- Etwa **300 Probanden** aus der Verwaltung eines der größten, europäischen Gesundheitszentren.
- Insgesamt **14** unterschiedliche **Artefakte**

STEIGERUNG DES SICHERHEITSBEWUSSTSEIN

SCHULUNGEN

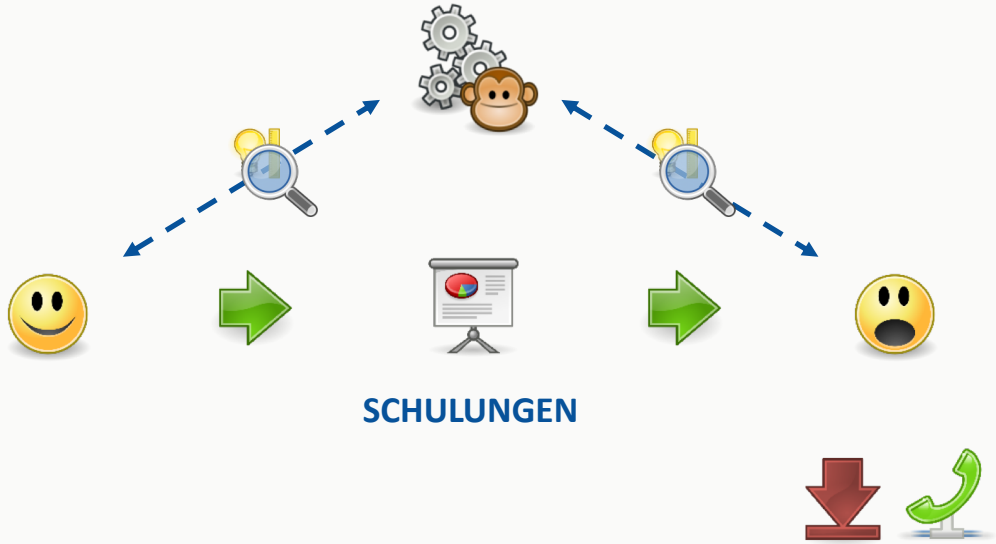
UNIVERSITÄT BONN

STEIGERUNG DES SICHERHEITSBEWUSSTSEIN



UNIVERSITÄT BONN

STEIGERUNG DES SICHERHEITSBEWUSSTSEIN



UNIVERSITÄT BONN

BESSER MESSEN, BESSER SCHÜTZEN