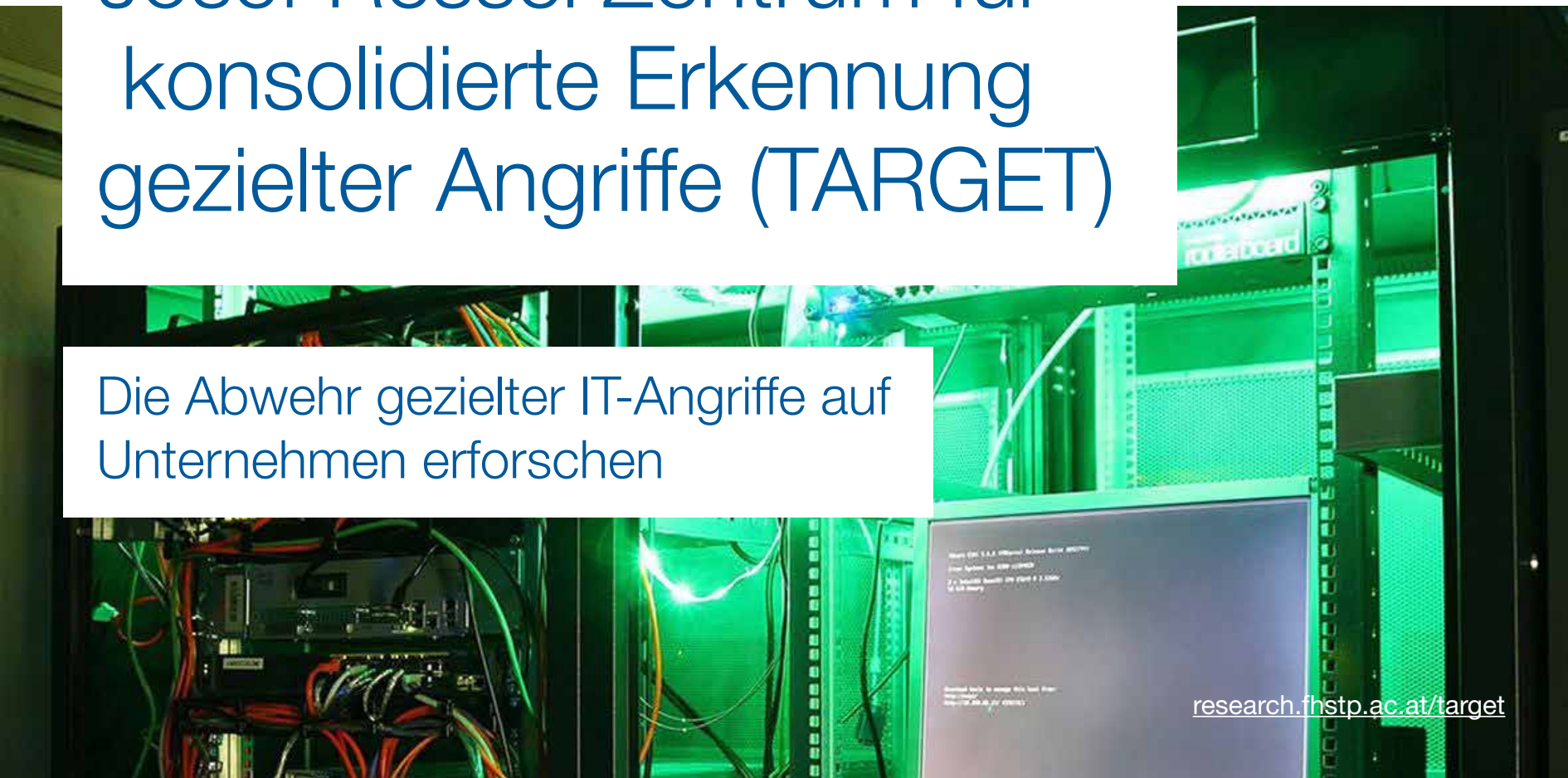
/informatik & security

/fh/// st.pölten

Josef Ressel Zentrum für konsolidierte Erkennung gezielter Angriffe (TARGET)



Die Abwehr gezielter IT-Angriffe auf Unternehmen erforschen

research.fhstp.ac.at/target

Das Josef Ressel Zentrum

für konsolidierte Erkennung gezielter Angriffe (TARGET)

Das Josef Ressel Zentrum für konsolidierte Erkennung gezielter Angriffe (TARGET) war eine Forschungseinrichtung an der FH St. Pölten. Es erforschte in den Jahren 2015 bis 2020 neue Techniken zur schnellen und sicheren Erkennung gezielter Angriffe auf IT-Systeme von Unternehmen und entwickelte eine ganzheitliche Methode zum besseren Verständnis und zur Abwehr dieser neuen Klasse an Cyber-Bedrohungen.

Wie erkennt man bisher unbekannte Angriffe?

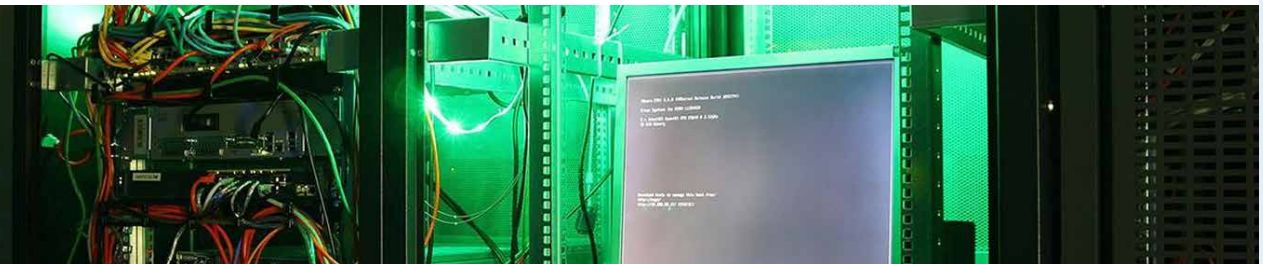
- Ein unbekannter IT-Angriff ist wie eine Nadel im Heuhaufen: Er geht in der großen Menge an normalen und alltäglichen IT-Aktivitäten unter.
- Um die Angriffe aufzuspüren, wurden am Resselzentrum TARGET verschiedene Ansätze von Data Science, IT-Security und künstlicher Intelligenz kombiniert, um die wenigen Angriffsaktivitäten vom großen Rest der normalen, harmlosen IT-Aktivitäten herauszufiltern und damit sichtbar und verständlich zu machen.

Wie lassen sich Angriffe beschreiben und einordnen?

- Angriffe können nach der Art des Angriffs, der Phase des Angriffs und den angegriffenen Systemen beschrieben werden.
- Im Resselzentrum TARGET wurden neuartige Methoden zum Klassifizieren und Beschreiben von möglichen Angriffen entwickelt. Sie helfen, neue und bisher unbekannte Angriffe schneller einzuordnen und geeignete Gegenmaßnahmen zeitnah treffen zu können.

Forschen gemeinsam mit Unternehmen

Firmenpartner im Zentrum waren die Unternehmen CyberTrap, SEC Consult, IKARUS Security Software und LG Nexera Business Solutions. SBA Research fungierte als wissenschaftlicher Partner in einem externen Modul des Zentrums.



Das Josef Ressel Zentrum TARGET wurde von der Christian Doppler Forschungsgesellschaft (CDG) und den beteiligten Firmenpartnern finanziert. Wir bedanken uns für die finanzielle Unterstützung durch das Bundesministerium für Digitalisierung und Wirtschaftsstandort und die Nationalstiftung für Forschung, Technologie und Entwicklung.

Personen und Stimmen

zum Josef Ressel Zentrum TARGET

„Das Josef Ressel Zentrum TARGET ist mit dem Ziel gestartet, zielgerichtete Angriffe schneller als bisher erkennen zu können und dabei auch die Vorgehensweise der Angreiferinnen und Angreifer zu verstehen. Die neuartigen Methoden, welche im Rahmen unserer Forschungstätigkeiten entstanden sind, ermöglichen eine Erkennung eines Angriffs in einer noch sehr frühen Phase und beschreiben dessen Kontext und mögliche Motivation auf verständliche Art und Weise.“

Sebastian Schrittwieser, Leiter des Josef Ressel Zentrums für konsolidierte Erkennung gezielter Angriffe (TARGET)

„Wir haben eine neuartige Technik entworfen, die es schafft, zielgerichtete Angriffe auf Servern rascher zu erkennen, etwa schon in der ersten Phase eines Einbruchs in ein IT-System, wo noch wenig Schaden entstanden ist, aber sich ein Angreifer oder eine Angreiferin bereits umsieht und das System analysiert.“

Martin Pirker, Senior Researcher, Department Informatik und Security, FH St. Pölten

„Mein Forschungsthema war, bösartige Prozesse von alltäglichen rasch unterscheiden zu können. Die Grenzen sind fließend – oft werden gute Prozesse bösartig missbraucht. Der Kontext macht jedoch den Unterschied.“

Sebastian Eresheim, Junior Researcher, Department Informatik und Security, FH St. Pölten

„Wir haben völlig neue Methoden entwickelt, die Angriffsmuster automatisch erkennen und gezielt Gegenmaßnahmen vorschlagen. So kann beispielsweise Betriebsspionage oder Sabotage besser entgegengewirkt werden.“

Robert Luh, FH-Dozent, Department Informatik und Security, FH St. Pölten

„Wir haben ein System entwickelt, welches es erlaubt Seitenkanäle bei der sogenannten Container-Virtualisierung automatisiert zu identifizieren. Dies kann unabhängig vom eigentlichen Betrieb solcher Lösungen erfolgen, um potentielle Probleme bereits im Vorfeld erkennen und die Sicherheitsregeln entsprechend anpassen zu können.“

Georg Merzdovnik, Senior Researcher SBA-Research

„Wir haben alle Aktivitäten eines jeden einzelnen Computers in einem Unternehmen aufgezeichnet und ein Programm entwickelt, das bei verdächtigen Aktivitäten sofort Alarm schlägt. Durch die gespeicherten Systemaktivitäten kann im Anschluss ein Angriff genau rekonstruiert werden.“

Helene Hochrieser, Junior Researcher, Department Informatik und Security, FH St. Pölten

Daten und Fakten

Josef Ressel Zentrum TARGET

Laufzeit:
5 Jahre

Gesamtbudget:
1,6 Mio. Euro

Entstandene Publikationen (Journal- und Konferenzbeiträge): **46**

- **Entstandene Diplom- und Bachelorarbeiten:** 15 bzw. 38
- **Co-Organisierte wissenschaftliche Konferenzen und Workshops:** 5
- **Bisher generiertes Projektvolumen aus Folgeförderungen:** ca. 650.000 Euro

Ausblick

- Unsere Forschung an gezielten IT-Angriffen geht weiter. Derzeit beschäftigen wir uns mit der systematischen Modellierung von Angriffen und den im jeweiligen Kontext besten Abwehrmaßnahmen
- Zwischen der FH St. Pölten und der Firma Cybertrap ist eine weitere Partnerschaft zum Thema Angriffsvisualisierung entstanden
- Die Firmenpartner arbeiten bereits an der Implementierung unserer Forschungsergebnisse in ihren Softwareprodukten

Forschung an der FH St. Pölten

Die FH St. Pölten ist eine forschungsstarke Hochschule. Wissenschaftler*innen forschen aktuell in sechs Instituten, einem zweiten Josef Ressel Zentrum und dem Center for Digital Health Innovation.

Mit den beiden Schwerpunktthemen Cyber Security & IT Security sowie Data Analytics & Visual Computing baut die FH St. Pölten in Interaktion mit regionalen, nationalen und internationalen Kooperationspartner*innen zielgerichtet Know-how und Ressourcen für eine digitale Gesellschaft aus.

Forschungsschwerpunkt Cyber Security & IT Security

Forscher*innen der FH St. Pölten entwickeln im Forschungsschwerpunkt „Cyber Security & IT Security“ neuartige Verfahren zum Erkennen, Interpretieren und Abwehren von IT-Angriffen, erforschen Grundlagen und neuartige Anwendungsgebiete von Blockchains in der IT-Sicherheit, sichern Industriesysteme durch innovative Konzepte ab und leisten wichtige Beiträge im Bereich Datenschutz und Privacy.

research.fhstp.ac.at

Kontakt Josef Ressel Zentrum TARGET:

Dipl.-Ing. Dr. Martin Pirker, Bakk.
Institut für IT Sicherheitsforschung
FH St. Pölten
T: +43/2742/313 228 690
E: martin.pirker@fhstp.ac.at
I: isf.fhstp.ac.at

JRZ TARGET JOSEF RESSEL CENTER FOR UNIFIED THREAT INTELLIGENCE ON TARGETED ATTACKS
Christian Doppler Forschungsgesellschaft
Bundesministerium Digitalisierung und Wirtschaftsstandort
FTE NATIONALSTIFTUNG FORSCHUNG | TECHNOLOGIE | ENTWICKLUNG