



Berner Fachhochschule
Institute for Cybersecurity and
Engineering ICE

Kommunikation

2501 Biel

Telefon 032 321 62 11

mediendienst.ti@bfh.ch
bfh.ch/ti

MEDIENMITTEILUNG

Biel, 1. Juni 2021

abuse.ch erhält neue Heimat an der BFH

abuse.ch, die weltweit bekannte und vielgenutzte Plattform zum Schutz vor Cyber-Bedrohungen, geht eine Partnerschaft mit der Berner Fachhochschule BFH ein. abuse.ch wird fortan als Forschungsprojekt am Institute for Cybersecurity and Engineering ICE betrieben. Der Verwaltung, Industrie und Forschung stehen dadurch weiterhin kostenlose Open Source-Daten sowie neue Möglichkeiten für die Bekämpfung von Cyber-Bedrohungen zur Verfügung.

Strafverfolgungsbehörden weltweit, wie das FBI oder das US Justice Department, haben bereits mit Hilfe von abuse.ch erfolgreiche Aktionen gegen Cyberkriminalität durchgeführt. Die zum Schutz von Cyber-Attacken rege genutzte Schweizer Non-Profit-Plattform ist in der internationalen IT-Community bekannt. In eigens initiierten Projekten hat abuse.ch bis heute über 1,2 Millionen Malware-Seiten identifiziert und unschädlich gemacht sowie über 40 Millionen Schadprogramme («Malware») analysiert. Nun geht die Community gesteuerte Plattform eine Partnerschaft mit der Berner Fachhochschule BFH ein und erhält am Institute for Cybersecurity and Engineering ICE ein neues Zuhause.

Zukünftig wird abuse.ch als BFH-Forschungsprojekt weiterbetrieben und entwickelt. «Mit abuse.ch verstärkt die BFH ihre Kompetenzen in den Bereichen Prävention, Erkennung und Analyse von Cyber-Bedrohungen», sagt Prof. Dr. Endre Bangerter, Co-Leiter des Institute for Cybersecurity and Engineering ICE. Wirtschaft und Behörden profitieren in Zukunft von neuen Projektmöglichkeiten und Dienstleistungen im Bereich Cybersicherheit mit der BFH. So wird abuse.ch weiterhin kostenlose Open Source Threat Intelligence zur Verfügung stellen, um die Verwaltung, Industriepartner und Hersteller von Sicherheitslösungen mit verlässlichen Daten zu versorgen. «Mit abuse.ch sind wir jetzt in der Lage, Netzwerke von Industriepartnern und deren Kundschaft in grossem Massstab effektiv vor Cyber-Bedrohungen zu schützen», so Dr. Bangerter.

Hinter abuse.ch steht Roman Hüsey, der das Projekt vor 15 Jahren gründete und seither führte. Er wird abuse.ch als wissenschaftlicher Mitarbeiter am ICE weiterbetreiben. Die BFH ermögliche der Community-gesteuerten Plattform einen weiterhin nicht-kommerziellen Betrieb, so Roman Hüsey. Mehr noch: «Als Forschungsprojekt erhält abuse.ch die nötigen Ressourcen, um sich weiterzuentwickeln und weitere Projekte im Bereich der Cybersicherheit in Angriff zu nehmen, die schlussendlich der Allgemeinheit zugutekommen», sagt Hüsey.

Kontakte

Prof. Dr. Endre Bangerter, Co-Leiter Institute for Cybersecurity and Engineering ICE, Berner Fachhochschule, endre.bangerter@bfh.ch, Tel. +41 32 321 64 78

Roman Hüsey, Wissenschaftlicher Mitarbeiter Institute for Cybersecurity and Engineering ICE, Berner Fachhochschule, roman.huessy@bfh.ch, Tel. +41 31 848 54 15

Michelle Buchser, Kommunikationsspezialistin, Berner Fachhochschule, Technik und Informatik, michelle.buchser@bfh.ch, Tel. +41 32 321 62 11

Weitere Informationen:

- [BFH-Projektseite](#)
- www.abuse.ch

abuse.ch

abuse.ch's Kernkompetenz ist die «Open Source Threat Intelligence». Der Begriff steht für Daten und Informationen zu Cyber-Bedrohungen, welche frei zur Verfügung gestellt werden. Diese Daten helfen Unternehmen und Organisationen, sich besser vor mögliche Cyber-Bedrohungen zu schützen. Zahlreiche Telekomanbieter, Unternehmen und Hersteller von IT-Sicherheitslösungen nutzen die von abuse.ch frei zur Verfügung gestellten Daten bereits heute, um eigene Netzwerke oder Kund*innen zu schützen. Durch den breitflächigen Einsatz dieser Daten erreicht abuse.ch direkt oder indirekt eine Vielzahl an Organisation und Internet-Users und trägt so seit der Gründung vor 15 Jahren weltweit massgeblich zur Cybersicherheit bei.

Behörden verwenden die abuse.ch-Daten für die Verbesserung der nationalen Internethygiene, indem beispielsweise Webseite, welche für die Verbreitung von Schadprogrammen («Malware») verwendet werden, aufgefunden und bereinigt werden. Auch die Justiz profitiert von abuse.ch: Strafverfolgungsbehörden weltweit verwenden abuse.ch zur Unterstützung bei Ermittlungen im Bereich Cyber-Kriminalität.

abuse.ch umfasst mehrere Community-gesteuerte Projekte. Eine Auswahl:

- **URLhaus:** Plattform mit Informationen zu Webseiten, welche von Cyberkriminellen für die Verbreitung von Schadprogrammen («Malware») verwendet werden.
- **MalwareBazaar:** Plattform, auf welcher IT-Sicherheitsforscher*innen Informationen zu aktuellen Schadsoftware («Malware») teilen können.
- **ThreatFox:** Plattform für den Austausch von technischen Informationen zu aktuellen Cyber-Bedrohungen (Indicators Of Compromise – IOCs).

Die Infrastruktur von abuse.ch besteht derzeit aus rund 55 Servern und 200 Sandboxes. Monatlich generiert das Projekt einen Netzwerkverkehr von über 130 TB und verarbeitet fast 300 Millionen HTTP-Anfragen. Pro Tag beantwortet abuse.ch rund zwei Millionen API-Anfragen und erzeugt 100 GB an komprimierten Daten.