TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

Neues aus dem EDUCV

Kurzvortrag auf der 27. DFN-Konferenz „Sicherheit in vernetzten Systemen“

Matthias Rack, Technische Universität Dresden, TUD-CERT

Hamburg, 24.02.2020

EDUCV?

- Arbeitsgruppe und Forum zu Themen der operativen Informationssicherheit an deutschen Hochschulen, Lehr- und Forschungseinrichtungen
- gegenseitige technische und politische Unterstützung bei Gründung von CERTs und CSIRTs an Universitäten, Hochschulen und Forschungseinrichtungen
- Erfahrungsaustausch und Weiterbildung der teilnehmenden Teams
- Unterstützung bei sicherheitstechnischen Analysen und Bewertungen
- Unterstützung bei Konzeption, Entwicklung und Betrieb von Sicherheitslösungen
- Erarbeitung und Veröffentlichung von Richtlinien, Handreichungen und Advisories

EDUCV - Mitglieder

- DFN-CERT, Hamburg
- KIT-CERT, Karlsruhe
- WWU-CERT, Münster
- RUS-CERT, Stuttgart
- GU-CERT, Frankfurt
- FUB-ART, Berlin
- TUD-CERT, Dresden

EDUCV - Aktivitäten 2019

Zwei Arbeitstreffen (Frühjahr / Herbst) - Themenauswahl:

- Arbeit an Handreichung für operative Sicherheitsteams (Fertigstellung geplant für Frühjahr 2020)
- Etablierung Chat-Plattform für EDUCV (Mitnutzung Mattermost-Instanz BSI / CERT-Bund)
- Integriertes Schwachstellenmanagement (Centreon, Greenbone SM)
- Sandboxing
- MISP
- Rollenspiel zu Incident Management und Incident Response
- Honeypots
- Netzwerksensoren
- DFN-SOC

EDUCV - kleine Statistik 2019

***„Incident-Charts“* der EDUCV-Mitglieder:**

1. Emotet (!), weitere Malware (E-Mail als Angriffsvektor)
2. Phishing
3. ausgenutzte Schwachstellen (vor allem Webanwendungen)

***Top-Themen* bei der Verbesserung der Informationssicherheit:**

1. Mailserver-Policies verschärfen (Legacy-Office-Dokumente / Makros)
2. 2FA
3. Ende von TLS 1.0 bzw. TLS 1.1
4. ISMS
5. Sandboxing
6. MISP

EDUCV - Mitglied werden?

Kriterien:

1. Angehöriger einer deutschen Hochschule, Lehr- oder Forschungseinrichtung
2. operatives Sicherheitsteam muss an Einrichtung existieren
3. Mitglied muss dem operativen Sicherheitsteam angehören
4. aktive Mitarbeit im EDUCV, Teilnahme an Arbeitstreffen

Aufnahme:

1. Empfehlung durch zwei EDUCV-Mitglieder (Veto-Recht für alle)
2. Gastteilnahme an Arbeitstreffen mit GHV (anschließend Veto-Runde)
3. formloser Antrag
4. EDUCV-Mitglied

Fragen?

- **Webseite**: https://www.educv.de
- **E-Mail:** info@educv.de