

ENISA-Bedrohungslandschaft: Unterstützung des Risikomanagements

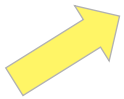
Louis Marinos| Bedrohungs-/Risikoanalytiker

Swiss Cyber Risk Research Conference 2016

Europäische Agentur für Netz- und Informationssicherheit

Bedrohungsintelligenz ist der Schlüssel für alle Sektoren des ISMS/Risikomanagements:

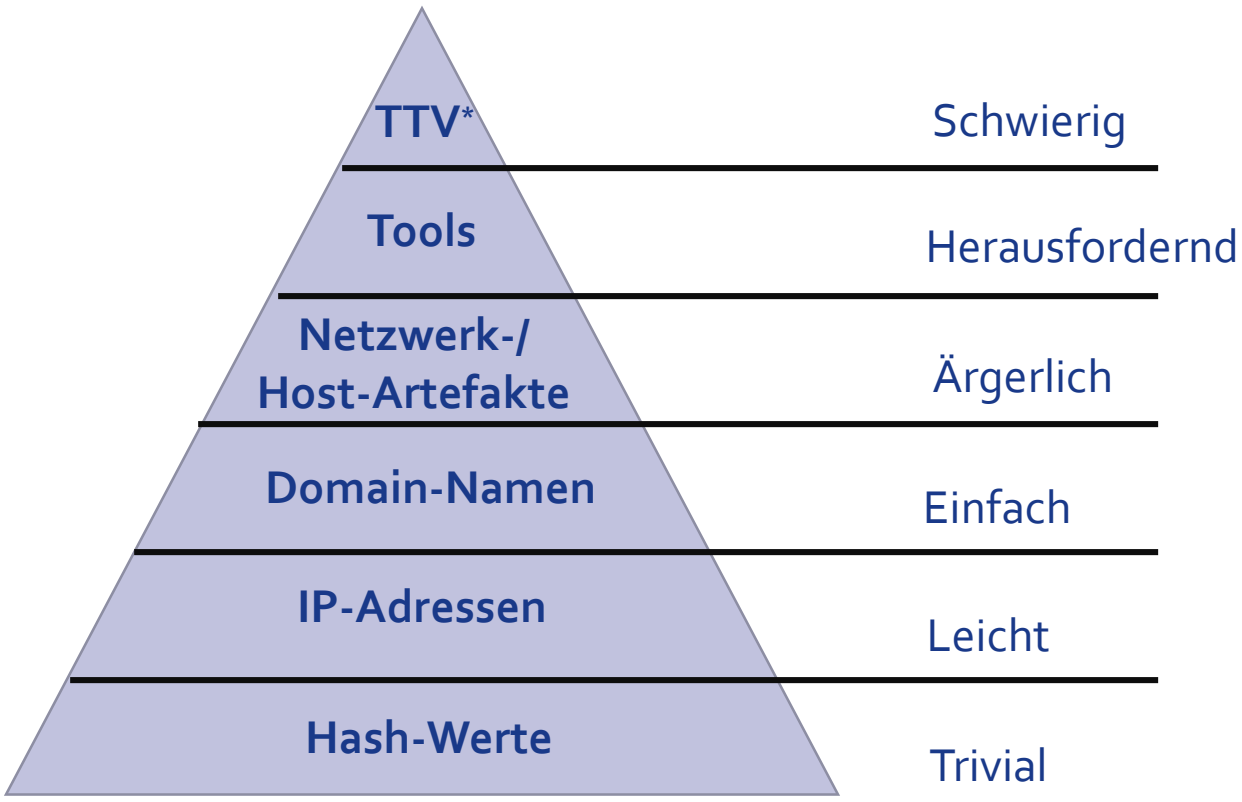
Dynamik

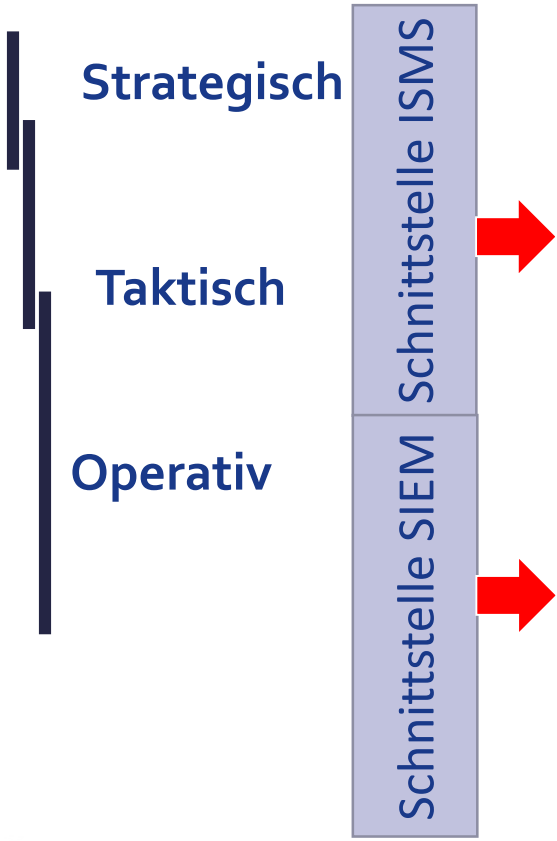
Risiko: [Asset, Verwundbarkeiten, Kontrollen] 

[Bedrohung, Bedrohungsagent] 

[Auswirkung, Wert, Einfluss] 

Bedrohungsdaten bilden eine Pyramide

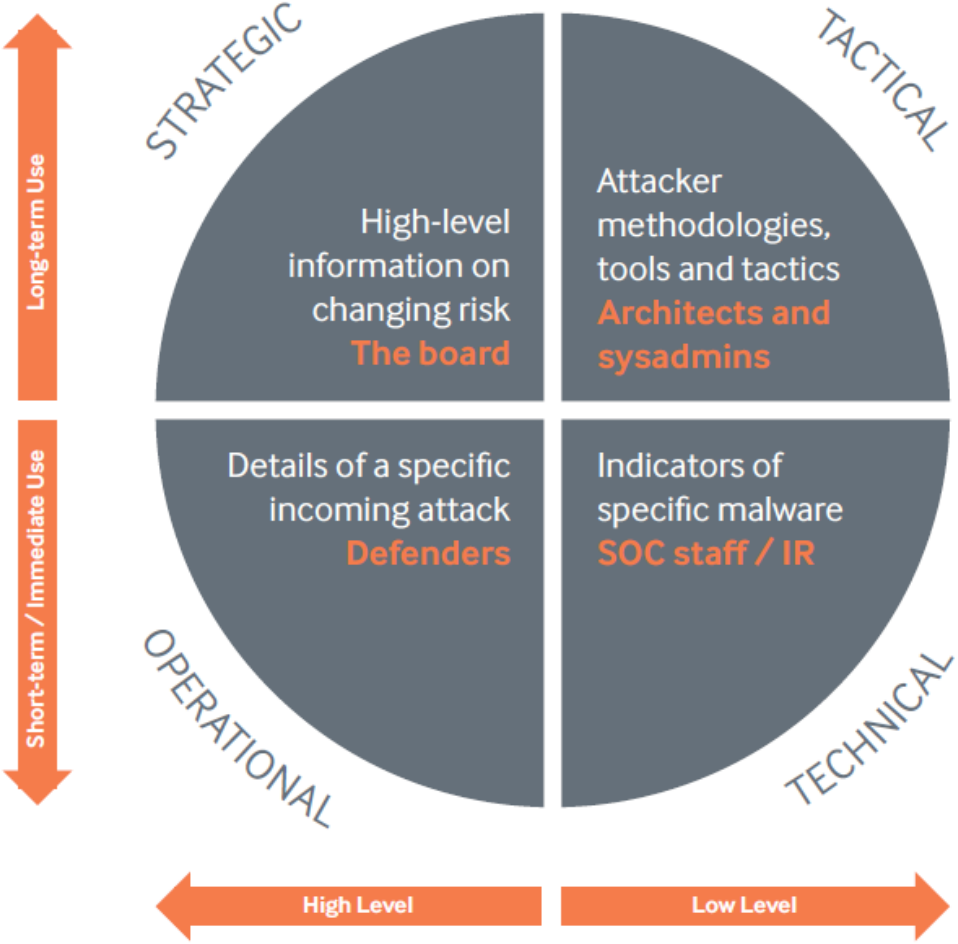




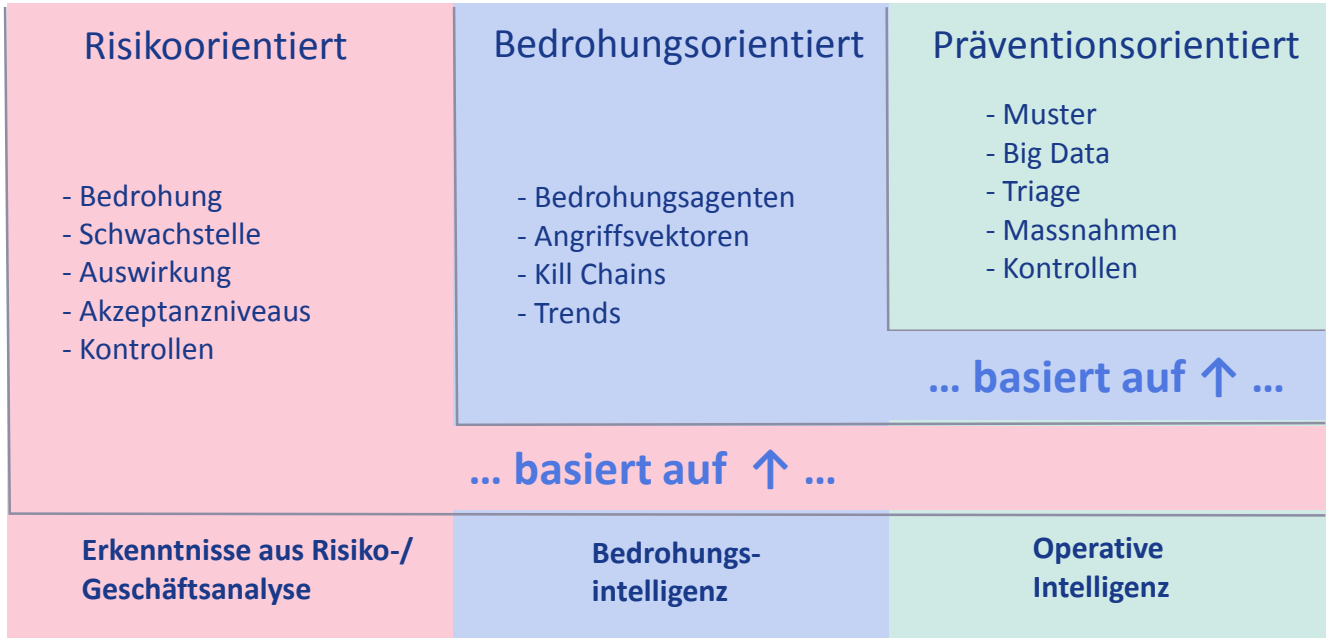
* TTV = Taktiken, Techniken und Verfahren

http://detect-respond.blogspot.gr/2013/03/the-pyramid-of-pain.html

Bedrohungslandschaft/Überblick über Bedrohungsintelligenz



Positionierung der Bedrohungsintelligenz



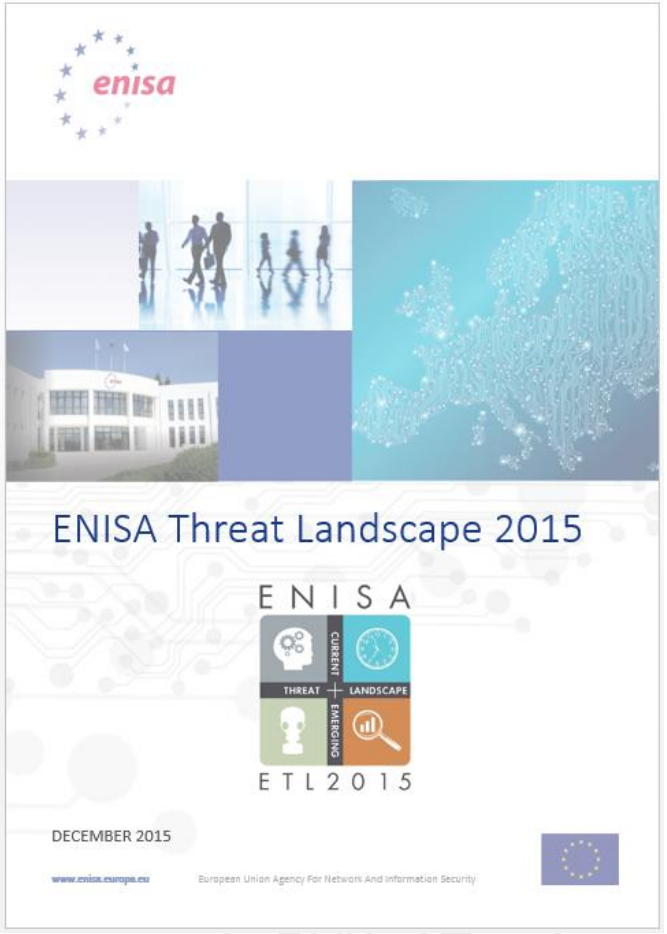
Wir müssen die Reaktionsgeschwindigkeit auf allen Ebenen ***erhöhen***!

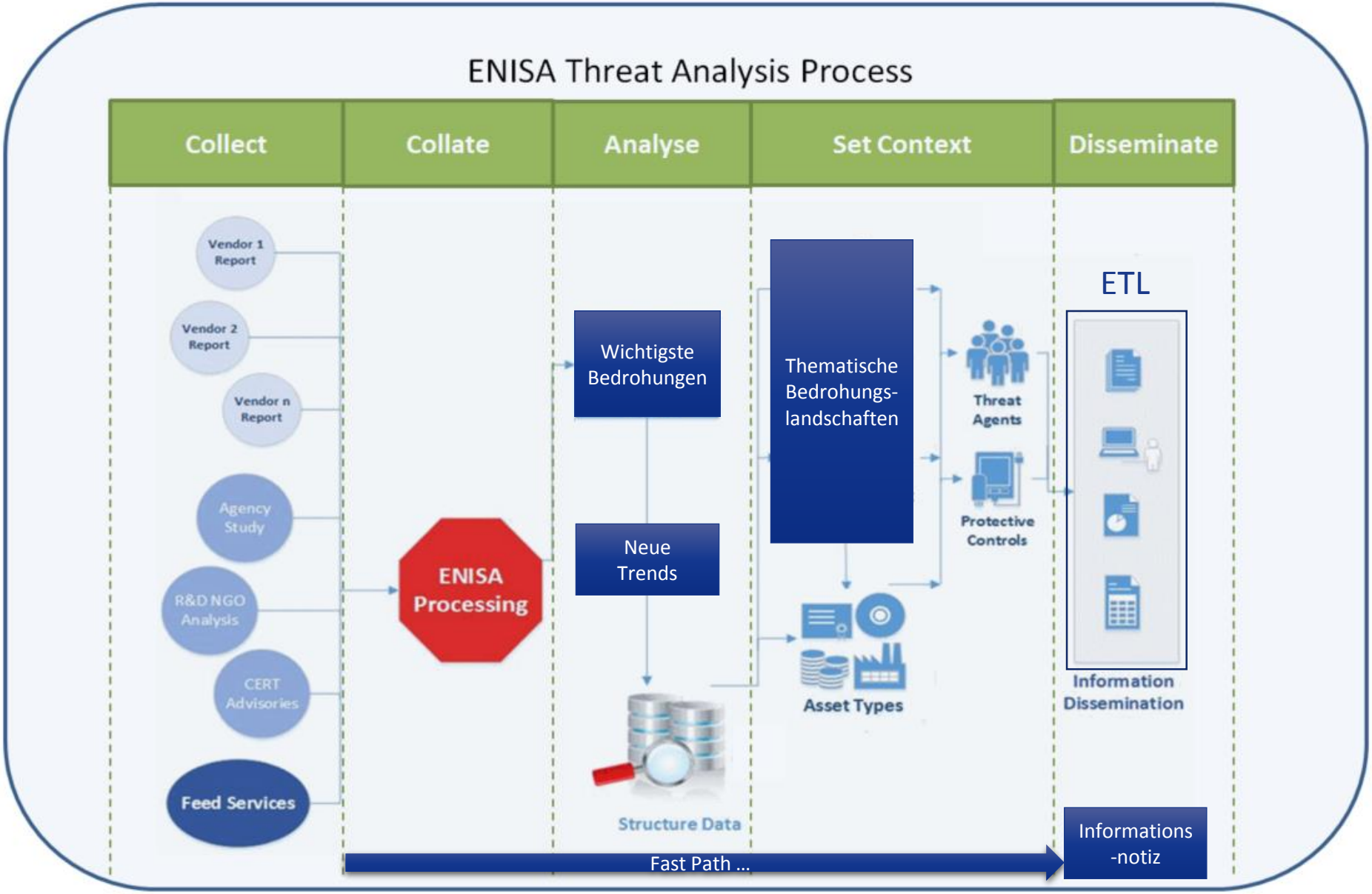
Die ENISA-Bedrohungslandschaft

Der ENISA-Bericht zur Bedrohungslandschaft vermittelt einen Überblick über die Bedrohungen sowie aktuelle und künftige Trends.

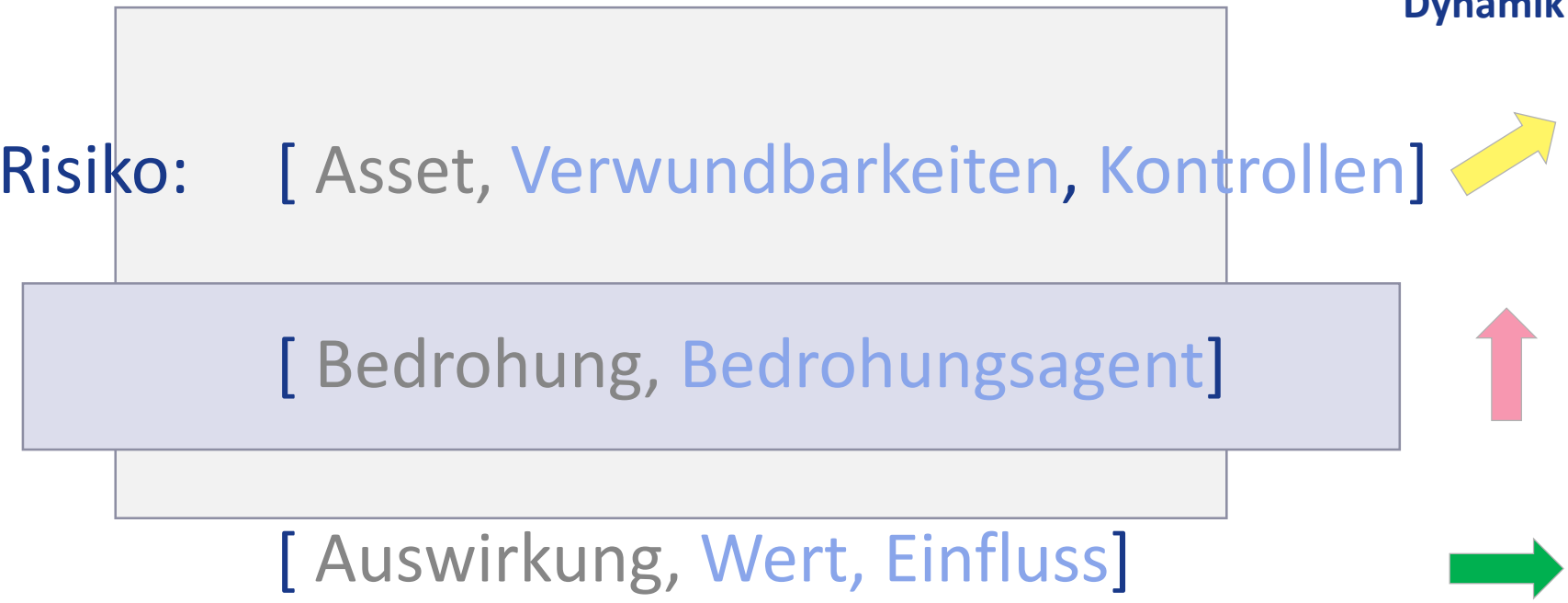
Er stützt sich auf öffentlich verfügbare Daten und bietet eine unabhängige Sicht auf die beobachteten Bedrohungen, Bedrohungsagenten und Bedrohungstrends.

Dazu wurden über 380 neue Berichte aus verschiedensten Quellen analysiert.




ENISA Threat Analysis Process
Collect
Collate
Analyse
Set Context
Disseminate
Vendor 1 Report
Vendor 2 Report
Vendor n Report
Agency Study
R&D NGO Analysis
CERT Advisories
Feed Services
ENISA Processing
Wichtigste Bedrohungen
Neue Trends
Structure Data
Thematische Bedrohungs-landschaften
Threat Agents
Protective Controls
Asset Types
ETL
Information Dissemination
Informations -notiz
Fast Path ...

Abgedeckte Themen:



Die wichtigsten Bedrohungen

Top Threats 2014	Assessed Trends 2014	Top Threats 2015	Assessed Trends 2015	Change in ranking
1. Malicious code: Worms/Trojans	↑	1. Malware	↑	→
2. Web-based attacks	↑	2. Web based attacks	↑	→
3. Web application /Injection attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Botnets	↓	→
5. Denial of service	↑	5. Denial of service	↑	→
6. Spam	↓	6. Physical damage/theft/loss	→	↑
7. Phishing	↑	7. Insider threat (malicious, accidental)	↑	↑
8. Exploit kits	↓	8. Phishing	→	↓
9. Data breaches	↑	9. Spam	↓	↓
10. Physical damage/theft /loss	↑	10. Exploit kits	↑	↓

HIGHLIGHTS: POSITIV

- Abgestimmte Massnahmen zur Beseitigung von schadhaften Infrastrukturen und zur Analyse von Vorfällen, um die Zuordnung der Täterschaft zu verbessern
- Stärkere Sensibilisierung der Regierungen, Erhöhung des Aufwands für Cyber-Abwehr, Ausbau der Fähigkeiten in diesem Bereich und Verbesserung der Kooperation zwischen Staaten
- Viele Entwicklungen in der Bedrohungsintelligenz: Erweiterung des Informationsaustauschs, Vermehrung der Instrumente und Produkte zur besseren Sensibilisierung sowie zur Verbesserung der Abwehrbereitschaft und -effienz
- F&E, um die bestehenden Schutzmassnahmen und -instrumente an die Veränderungen in der Cyber-Bedrohungslandschaft anzupassen

HIGHLIGHTS: WENIGER POSITIV

- Anhaltende Hardware-basierte Angriffe, weit unterhalb des «Radars» der verfügbaren Abwehrinstrumente und -methoden
- Ausbau des Geschäftsfeldes «Cyber Crime as a Service», Tool-Entwicklungen für Nicht-Experten und Partnerprogramme
- Hocheffiziente Bewaffnung mit schadhafter Software (Malware) und Infektions-Tools, die sich auf erkannte Schwachstellen abstützen
- Hochprofitabler Betrieb von schadhaften Infrastrukturen und Malware-Kampagnen, um Daten zu missbrauchen und zu erpresserischen Zwecken zu verschlüsseln (Ransomware)

SCHLUSSFOLGERUNGEN FÜR DIE POLITIK

- Bedrohungsintelligenz zu einem festen Bestandteil der nationalen Cyber-Abwehrsysteme machen
- Gemeldete Vorfälle analysieren und die Ergebnisse für eine bessere Planung der Abwehr verwerten
- Wissen rund um Cyber-Bedrohungen an alle Beteiligten im Cyberspace weitergeben

SCHLUSSFOLGERUNGEN FÜR DIE INDUSTRIE

- Inhalt von Bedrohungsintelligenz vereinfachen, um eine grössere Verbreitung dieser Informationen in allen interessierten Kreisen zu erreichen
- Modelle von Bedrohungsagenten detaillierter ausarbeiten und zu einem festen Bestandteil der Bedrohungsintelligenz machen
- Korrelierte, in den Gesamtzusammenhang eingeordnete Bedrohungsdaten ermitteln, um die Dauer ihrer Relevanz zu erhöhen
- In ein besseres Management der Verwundbarkeiten und die Ausnutzung des Darknets investieren

SCHLUSSFOLGERUNGEN FÜR DIE FORSCHUNG

- Angewandte statistische Modelle entwickeln, um die Vergleichbarkeit von Cyber-Bedrohungen und von Informationen über Vorfälle zu verbessern
- Neue Modelle für nahtlos betriebene Sicherheitskontrollen entwickeln, die in komplexe, intelligente Endanwender-Umgebungen integriert werden
- Vertrauensmodelle für die Ad-hoc-Interoperabiliät von Geräten in intelligenten Umgebungen entwickeln

Sicherheitsfachleute: INNOVATION IST GEFRAGT!

- Bedrohungsintelligenz am richtigen Ort ermitteln
  (in Unternehmen jeder Grösse ermöglichen)
- Grundsätze zur Identifizierung der Bedrohungslandschaft anwenden
  (Risiken, Assets, Schutz)
- Bedrohungslandschaft nutzen, um den Schutz zu testen
  (Realität simulieren)

Danke für Ihre Aufmerksamkeit!

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu