Bedeutung von OSINT

Cyber Threat Intelligence
im Zusammenhang mit Cyber Security für Unternehmen

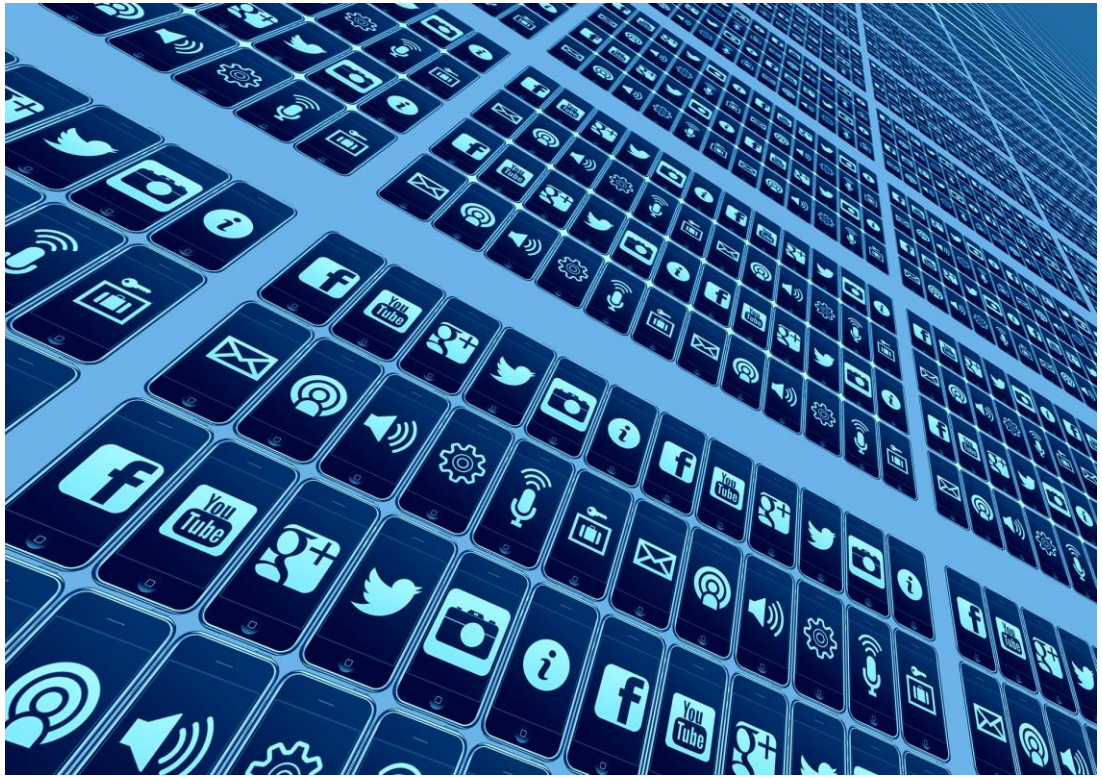
Günter Aigle ©
Dipl. Ing. (BA)
CISSP, Lead Auditor 27001 (PECB)

Agenda

- „Cyber-Bedrohungen“ – die Hintergründe und Ursachen
- Kurzer Einblick in die aktuelle Bedrohungslage
- Bedeutung von OSINT für potentielle Angreifer
- OSINT Werkzeuge
- „Kennen Sie Ihr Cyber-Risiko?“
- OSINT – Abwehr- und Schutzmechanismen

Günter Aigle ©
Dipl. Ing. (BA)
CISSP, Lead Auditor 27001 (PECB)

Das Internet…



unendliche Weiten…

Günter Aigle ©
Dipl. Ing. (BA)
CISSP, Lead Auditor 27001 (PECB)

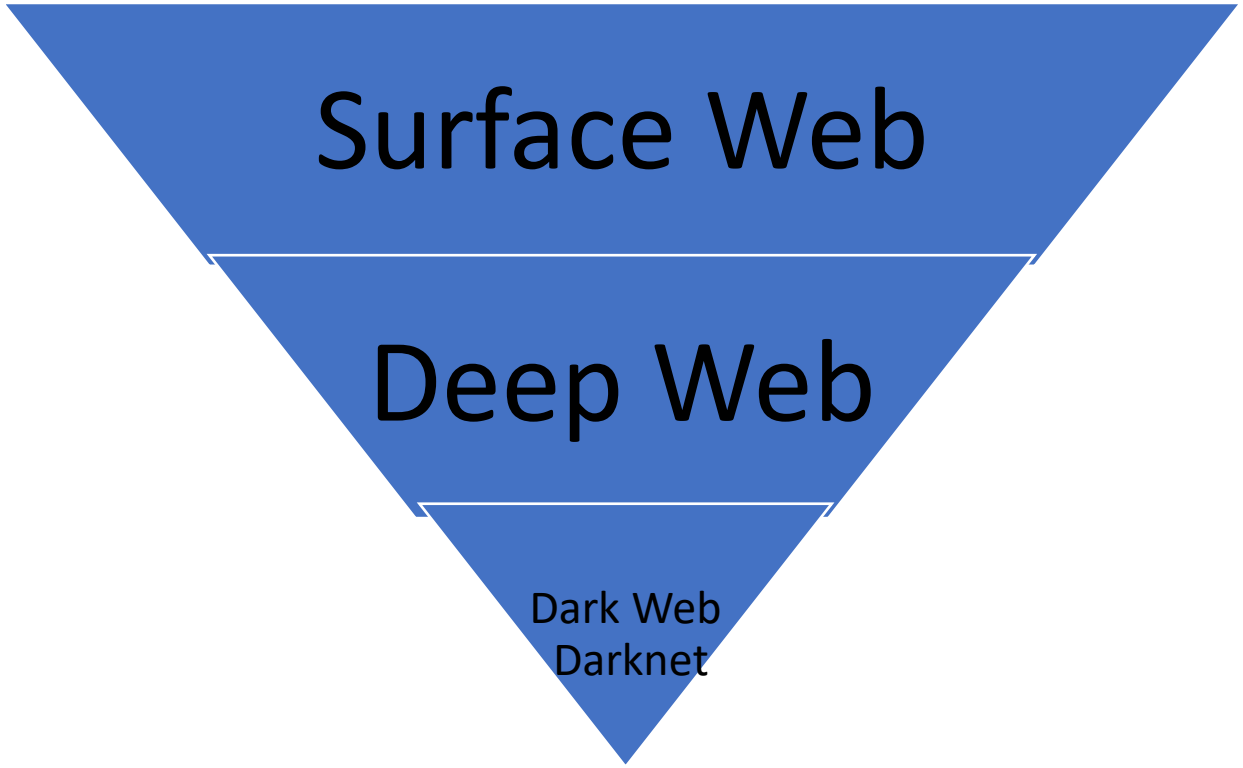
Jede Minute…

- in nur einer Minute landen Million über Millionen Informationen im Internet
- z.B. werden in nur 60sec. ca. 200 Millionen versendet
- auf YouTube werden in nur einer Minute 500 Stunden Inhalte hochgeladen
- 200.000 Menschen versenden Tweets auf Twitter
- ca. 9000 Menschen verlinken sich auf LinkedIn

Günter Aigle ©
Dipl. Ing. (BA)
CISSP, Lead Auditor 27001 (PECB)

Mit dieser unglaublichen Menge an Daten…

- Entsteht im Internet ein Mark für Daten, welcher zunehmend wächst

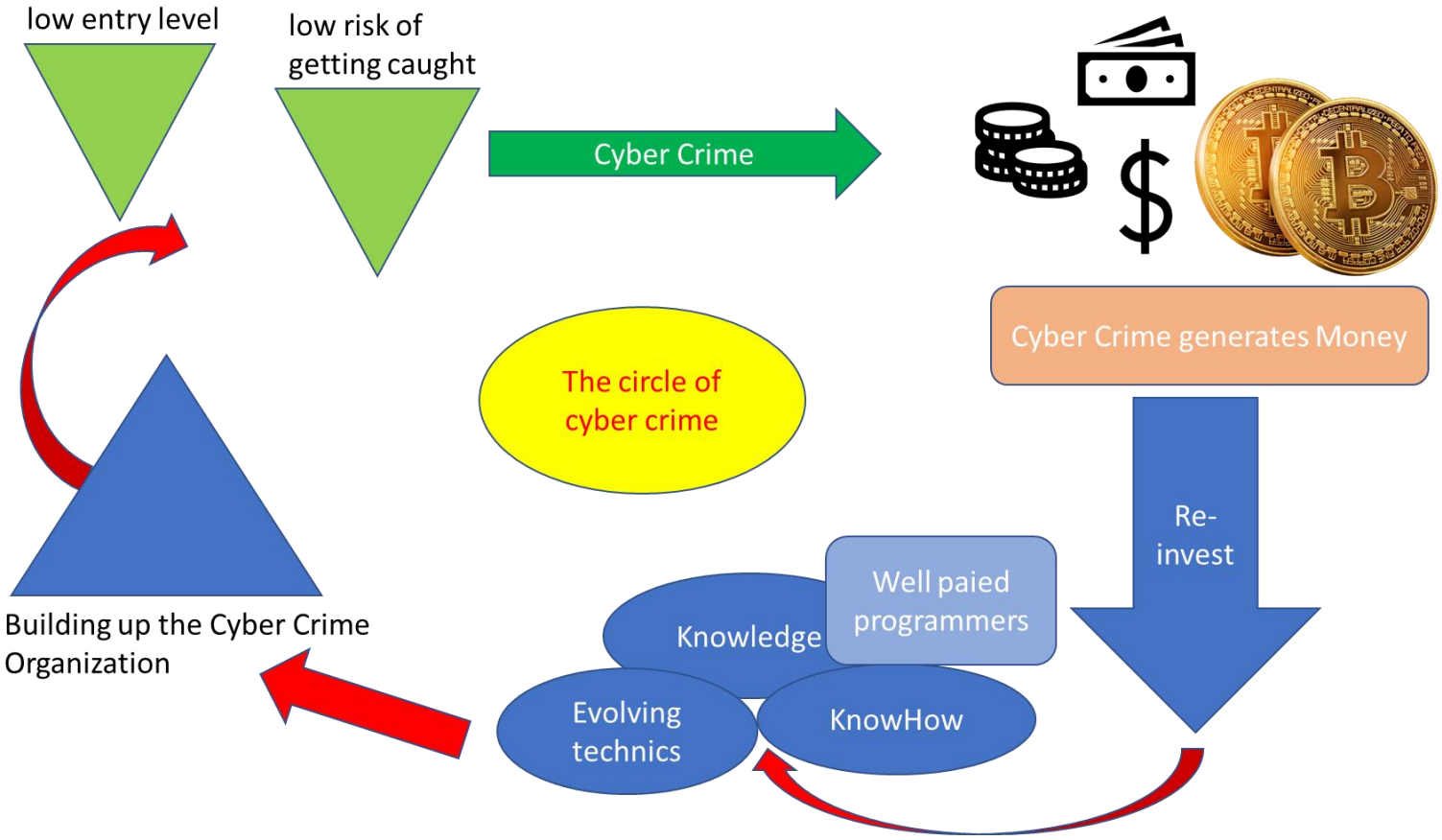


Günter Aigle ©
Dipl. Ing. (BA)
CISSP, Lead Auditor 27001 (PECB)

Die Menge der Information…

…beflügelt das Verbrechen: Cyber Crime ist „en vogue“

Günter Aigle ©
Dipl. Ing. (BA)
CISSP, Lead Auditor 27001 (PECB)



Längst mehr als nur ein Geschäftsmodell:
Die Cyber Crime „Industrie“

Global agieren zig Gruppen:
Cobalt, Lazarus, MegaCart, Evil Group, GozNym, Darkside, REvil, Clop, SyrianElectronicArmy, FIN7, ...

Politik und Cyber Crime vermischen sich

Günter Aigle ©
Dipl. Ing. (BA)
CISSP, Lead Auditor 27001 (PECB)

Es ist nicht eine Frage, ob man angegriffen wird…

…sondern nur noch eine Frage von: „wann und auf welche Art und Weise!“

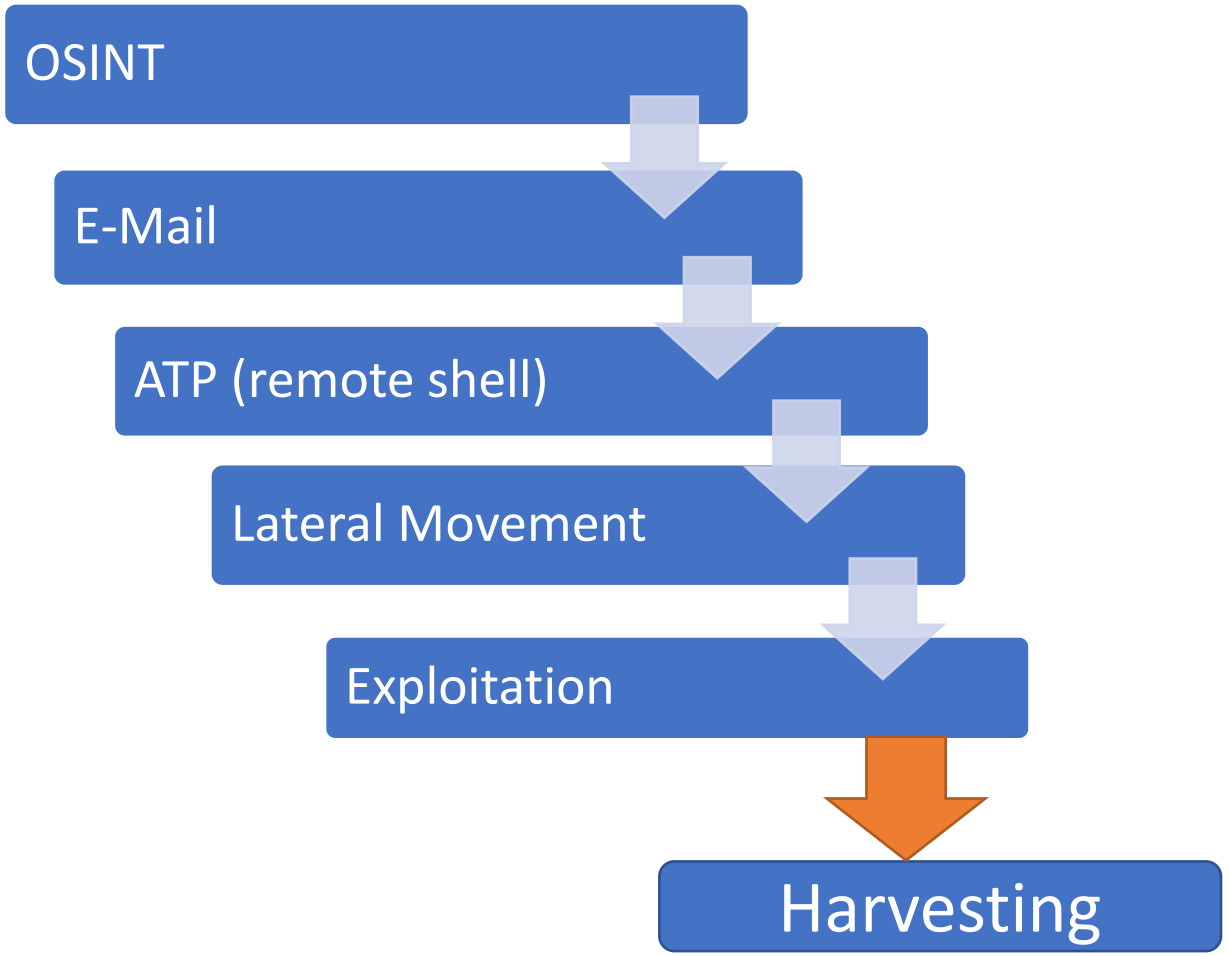
Günter Aigle ©
Dipl. Ing. (BA)
CISSP, Lead Auditor 27001 (PECB)

Jeder klassische Einbruch…

…beginnt mit dem Auskundschaften!

Günter Aigle ©
Dipl. Ing. (BA)
CISSP, Lead Auditor 27001 (PECB)

Cyber Kill Chain



Günter Aigle ©
Dipl. Ing. (BA)
CISSP, Lead Auditor 27001 (PECB)

OSINT „Footprinting“ (Reconnaissance)

- Aus dieser riesigen Informationsmenge kann man nun jede Menge Information filtriert und gewonnen werden:
  - E-Mail Adressen
  - IP-Adressen
  - Domains und Sub-Domains
  - Zugänge wie OWA oder Citrix
  - …

Günter Aigle ©
Dipl. Ing. (BA)
CISSP, Lead Auditor 27001 (PECB)

OSINT – Tools (Maltego)

- OSINT – Tools wie Maltego liefern eine visuelle Korrelation dieser Informationen
- https://www.maltego.com/
- SATAYO ist ebenfalls ein mächtiges, relativ einfach zu bedienendes OSINT – Tool -> einige Screenshots finden Sie auf den folgenden Folien

Günter Aigle ©
Dipl. Ing. (BA)
CISSP, Lead Auditor 27001 (PECB)

OSINT in Action (SATAYO)

Collection #1

Unverified breach, may be sourced from elsewhere

In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popu
hacking forum. The data contained almost 2.7 *billion* records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on
the incident and how to search the breached passwords are provided in the blog post The 773 Million Record "Collection #1" Data Breach.

Breach Date: 2019-01-07
Last update for this domain: **2020-08-25**
Compromised accounts: 772,904,991
Compromised data: Email addresses, Passwords

Spread: widespread
Typology: very critical data
Complexity: no element of complexity [ex. plaintext password]

9 months ago
9 months ago
9 months ago

Exploit.In

Unverified breach, may be sourced from elsewhere

In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different
passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the
account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.

Breach Date: 2016-10-13
Last update for this domain: **2020-08-25**
Compromised accounts: 593,427,119
Compromised data: Email addresses, Passwords

Spread: widespread
Typology: very critical data
Complexity: no element of complexity [ex. plaintext password]

9 months ago

Anti Public Combo List

Unverified breach, may be sourced from elsewhere

In December 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Anti Public". The list contained 458 million unique email addresses, many with multiple
different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems
where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.

9 months ago

Günter Aigle ©
Dipl. Ing. (BA)
CISSP, Lead Auditor 27001 (PECB)

OSINT PWD (SATAYO)

Count	Password	Password decrypt	Mail
3	l[redacted]		[redacted]
1	sha1 74b579a5d3d5007916b1373d123c7ca011e59801	f973ceeb47	
1	sha1 f4b40225275c8deccdab050e3658ca3fb284c857	No result found in our database	
1	Patrick123		

Count	Password	Password decrypt
3	79846c52[redacted]	
3	b8ewK	
3	cac0	
3	tasc[redacted]	
3	wi[redacted]	
2	3K14CRQK	
2	esibqphj	
2	fokujiwo	
2	Oxylog	
2	tilli1	

Günter Aigle ©
Dipl. Ing. (BA)
CISSP, Lead Auditor 27001 (PECB)

Und wieviel Information…

…gibt es da draußen über SIE und IHR Unternehmen?

Günter Aigle ©
Dipl. Ing. (BA)
CISSP, Lead Auditor 27001 (PECB)

OSINT – Abwehr- und Schutzmechanismen

- Ermittlung des Cyber-Risikos
- Aufklärung: Security Awareness
- Cyber Hygiene: „das Internet muss nicht alles wissen“
- Ermittlung der eigenen Schwachstellen (Pentests)
- Besonderer Schutz der „Kronjuwelen“

Günter Aigle ©
Dipl. Ing. (BA)
CISSP, Lead Auditor 27001 (PECB)

Thank you for your ATTENTION

Vielen Dank für Ihre Aufmerksamkeit

Muchas gracias por su atención

Günter Aigle ©
Dipl. Ing. (BA)
CISSP, Lead Auditor 27001 (PECB)