T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

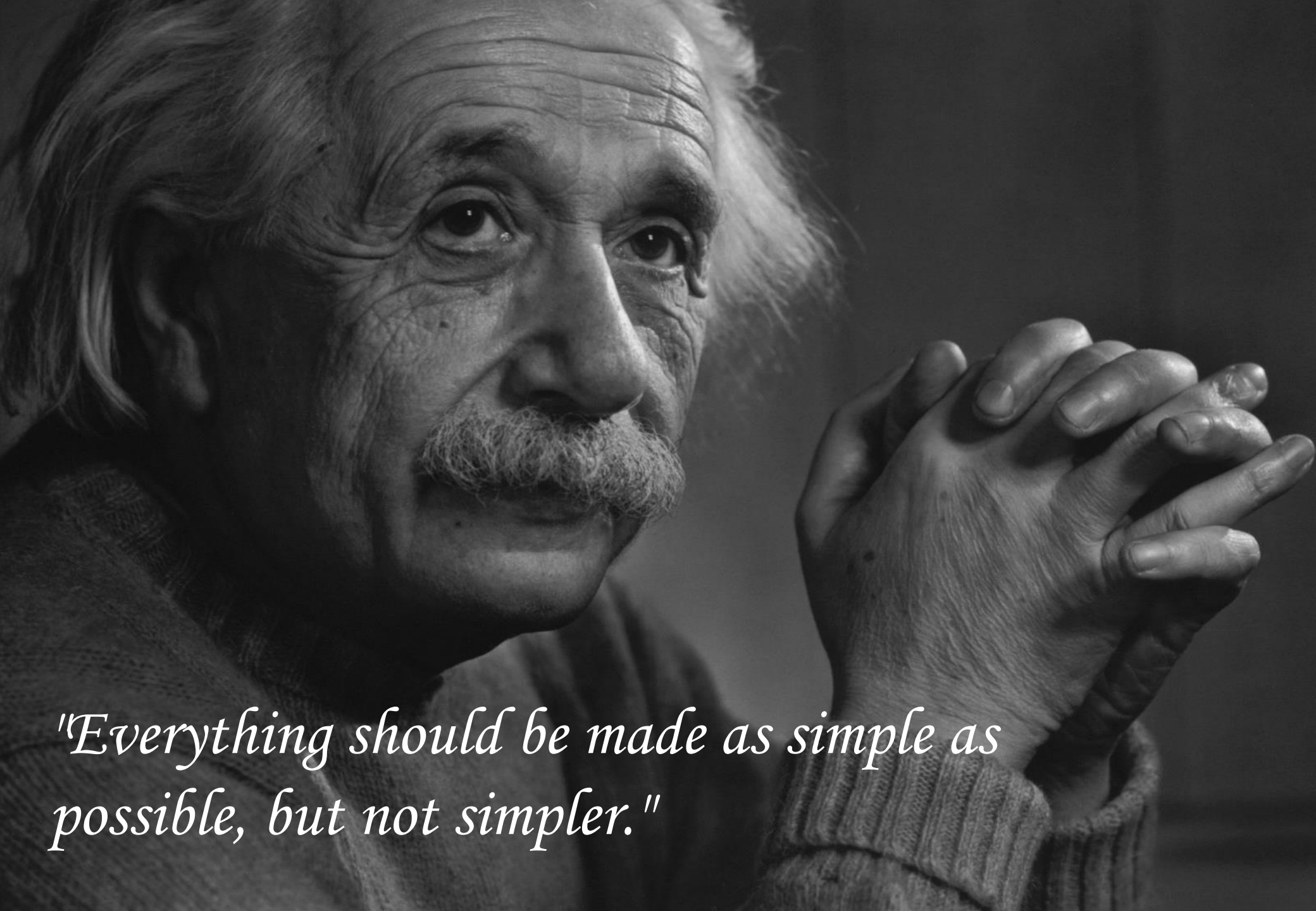
T.I.S.P. Community Meeting

Berlin, 02. - 03.11.2015

Index der Gefährdungslage

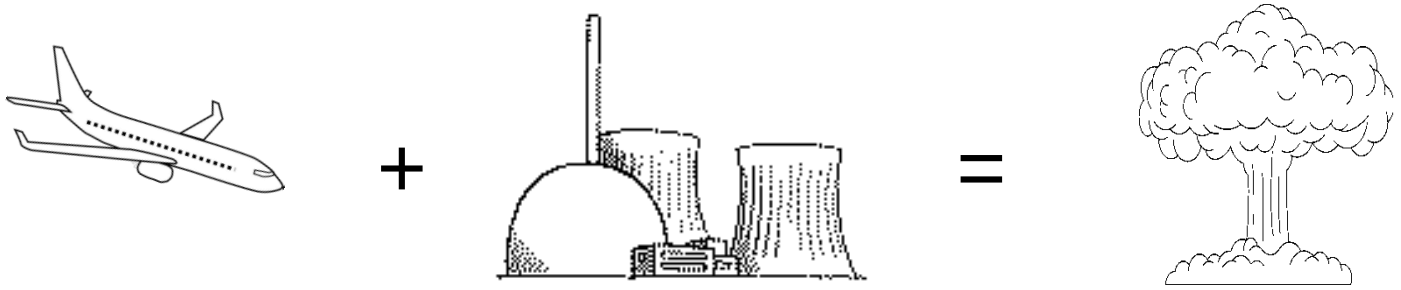
Holger Himmel

Tengelmann WHG KG


"Everything should be made as simple as possible, but not simpler."

Grundlagen

Bedrohung + Verwundbarkeit = Gefährdung

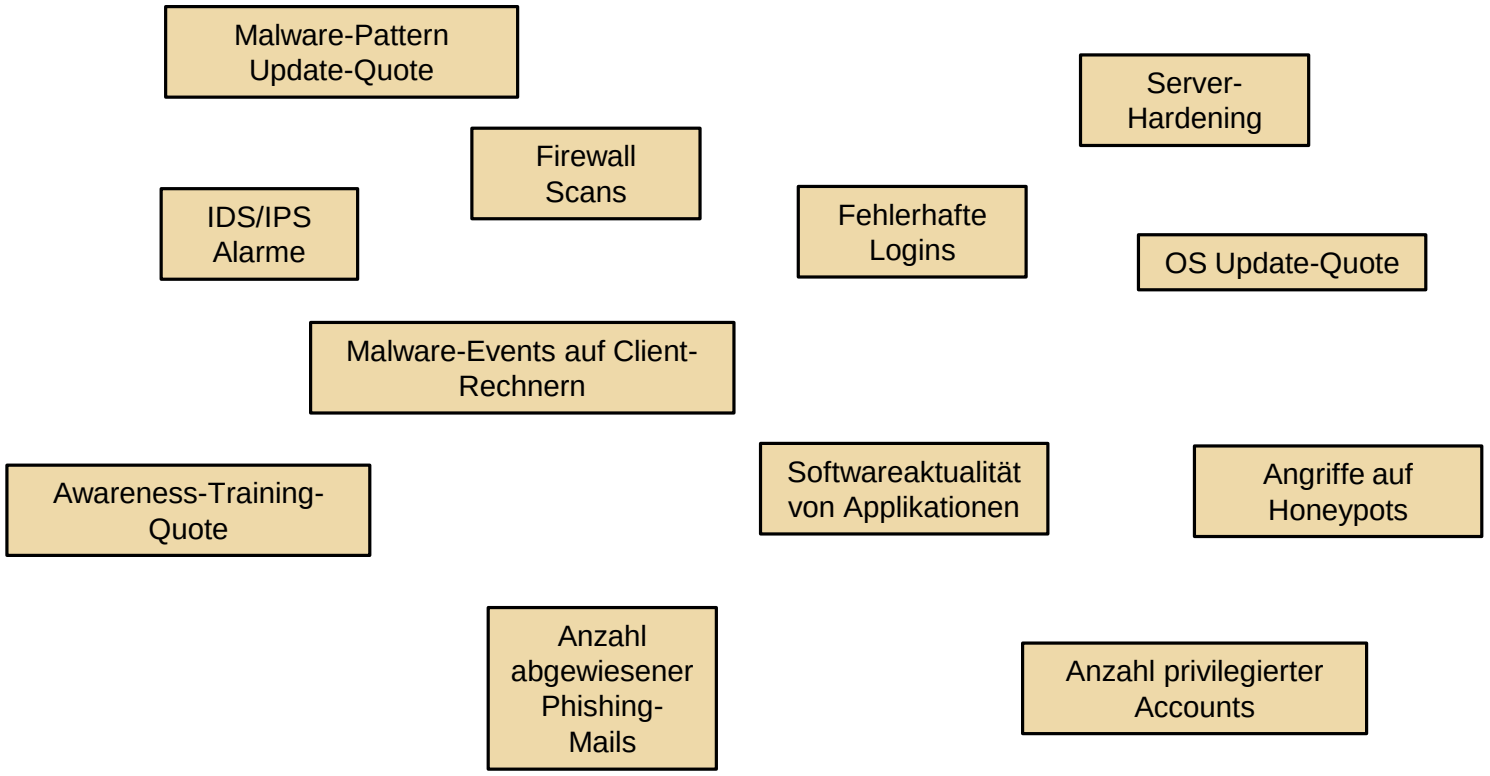


Hacker + Schwache Verschlüsselung = Datendiebstahl

Index der Bedrohungslage + Index der Verwundbarkeit = Index der Gefährdungslage

1. Metriken sortieren

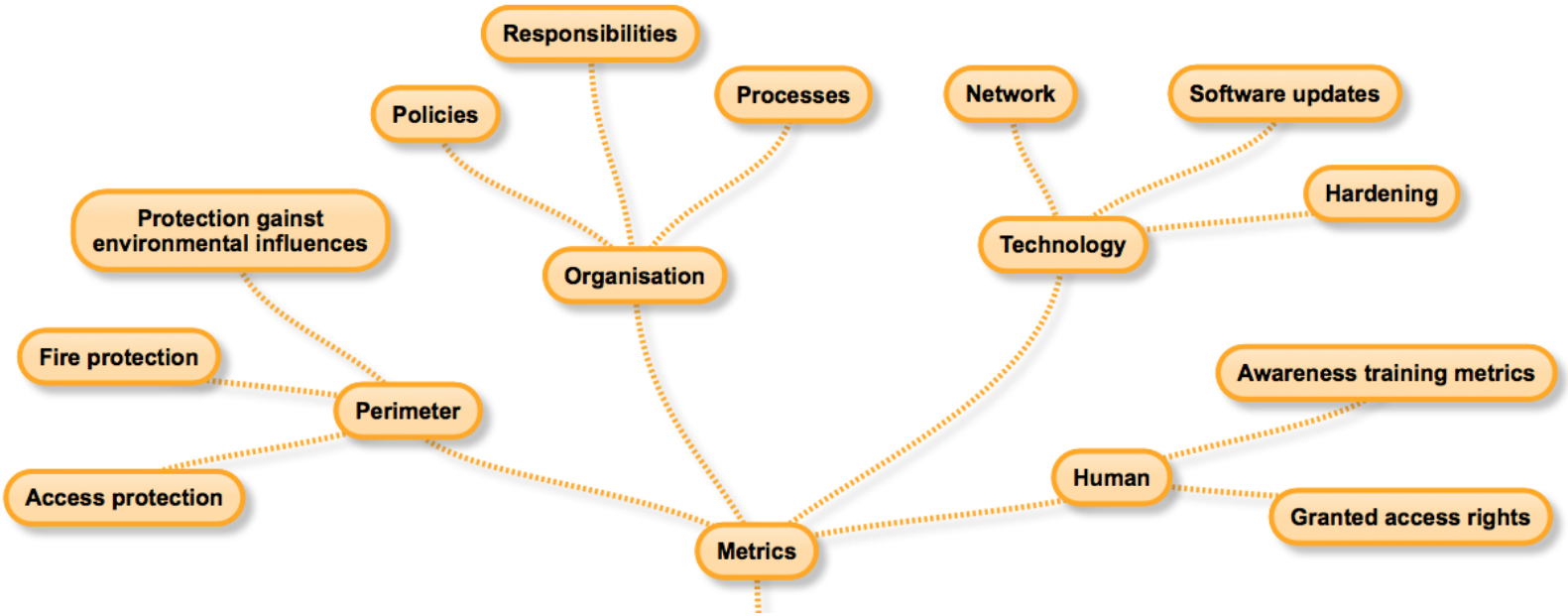
Frage: Misst eine Metrik eine Verwundbarkeit oder eine Bedrohung?



Es gibt hunderte mehr davon…

1. Metriken sortieren

Verwundbarkeits-Metriken lassen sich wie folgt clustern:



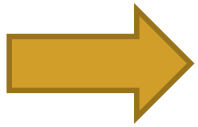
"[…] the most important figures that one needs for management are unknown or unknowable […], but successful management must nevertheless take account of them." - W. Edwards Deming

2. Index der Verwundbarkeit

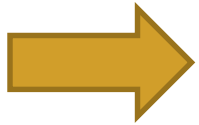
1. Normalisieren

Was bedeutet es, wenn (irgendeine) Metrik "89,2%" oder "1.630" anzeigt?
Ist das gut oder schlecht?

Normalisierung setzt eine Metrik in ***Ihren*** Kontext und lässt ***Sie*** definieren was "*gut*" und was "*schlecht*" ist.

"89,2%" 

Normskala	
80,00%	10
82,00%	9
84,00%	8
86,00%	7
88,00%	6
90,00%	5
92,00%	4
94,00%	3
96,00%	2
98,00%	1
100,00%	0

 "6"

2. Index der Verwundbarkeit

2. Gewichten

Es gibt Metriken, die sind "*wichtiger*" oder "*aussagekräftiger*" als andere. Sie zu gewichten gibt ***Ihnen*** die Möglichkeit dies bei der Berechnung des Index zu berücksichtigen.

Zur Vereinfachung geben wir *"normal"* eine Gewichtung von "1".

				Normskala										
	Wert	**Norm.**	**Gewichtung**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Metrik 1	100,00%	0	1	X										
Metrik 2	92,70%	8	2									X		
Metrik 3	80,00%	1	1		X									
Metrik 4	99,70%	2	1			X								
Metrik 5	99,00%	1	1		X									
Metrik 6	80,10%	4	1					X						

2. Index der Verwundbarkeit

3. Den Score berechnen

Formel:

$$Score(S) = \sum_{1}^{Metrik\ n} (Normwert(N) \cdot Gewichtungsfaktor(W))$$

	Wert	Norm.	Gewichtung	Normskala 0	1	2	3	4	5	6	7	8	9	10
Metrik 1	100,00%	0	1	X										
Metrik 2	92,70%	8	2									X		
Metrik 3	80,00%	1	1		X									
Metrik 4	99,70%	2	1			X								
Metrik 5	99,00%	1	1		X									
Metrik 6	80,10%	4	1					X						

Score = 0 · 1 + 8 · 2 + 1 · 1 + 2 · 1 + 1 · 1 + 4 · 1 = **24**

2. Index der Verwundbarkeit

4. Den Indexwert berechnen (in %)

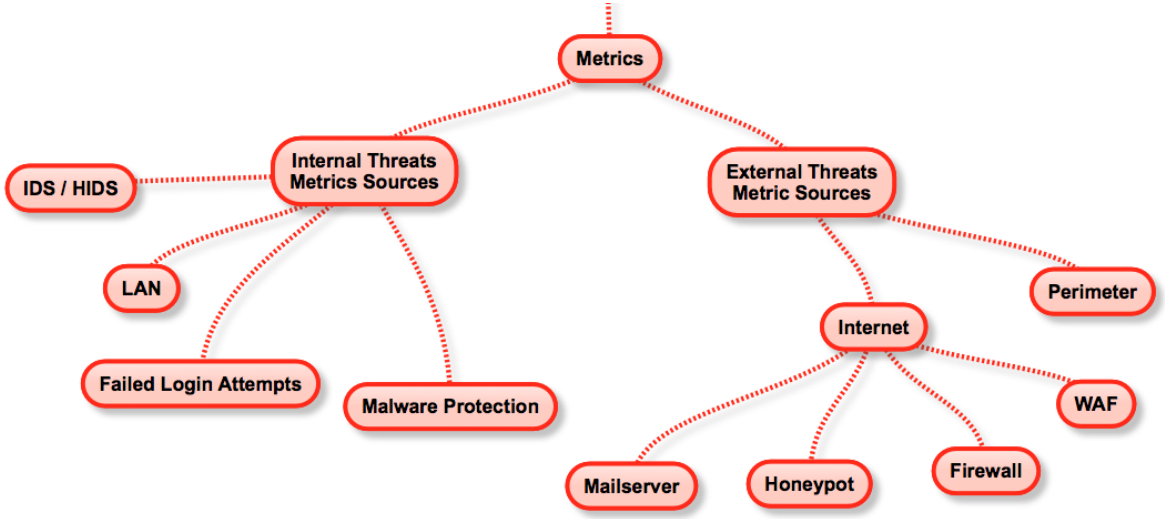
Formel:

$$Index\ der\ Verwundbarkeit = \frac{Score}{\sum_{1}^{Metrik\ n}(MaxNormwert(V)\ \cdot Gewichtungsfaktor(W))} \cdot 100$$

	Wert	Norm.	Gewicht	Normskala 0	1	2	3	4	5	6	7	8	9	10	
Metrik 1	100,00%	0	1	X											10
Metrik 2	92,70%	8	2									X			20
Metrik 3	80,00%	1	1		X										10
Metrik 4	99,70%	2	1			X									10
Metrik 5	99,00%	1	1		X										10
Metrik 6	80,10%	4	1					X							10
		Score	**24**												**70** (=100%)

3. Index der Bedrohungslage

Metriken der Bedrohungen clustern:



Alle Bedrohungsmetriken haben eine Sache gemeinsam: Sie können sie nicht beeinflussen.

"Blocked Phishing-Mails" ist ein Beispiel hierfür. Man kann keinen Soll-Wert im Sinne von "Nächsten Monat möchte ich bitte nur 1 Mio. geblockte Mails haben" setzen.

Bei Verwundbarkeits-Metriken kann man dies sehr wohl:
"Nächsten Monat sollen meine Malware-Pattern zu 100% aktuell sein!".

3. Index der Bedrohungslage

1. Normalisieren (Schon schwieriger …)

Beispiel: Sie hatten letzten Monat 200.000 Phishing-Mails geblockt.
Gut oder schlecht?

Wenn Sie in der Vergangenheit im Durchschnitt 6.000.000 geblockte Mails pro Monat hatten ist das "gut". Hatten sie nur 4.000 im Durchschnitt pro Monat ist das schon fast "worst case".

Bedrohungsmetriken in einen historischen Kontext zu stellen scheint also *eine* Lösung zu sein.

3. Index der Bedrohungslage

1. Normalisieren

Eine Möglichkeit: Man nehme die 3/4/5 Maximalwerte der letzten 12/52 Perioden und bilde den Durchschnitt. Das ist ***Ihr*** "worst case" (10) in ***Ihrer*** Normskala.

Beispiel: Sie haben diese 12 Werte aus der Vergangenheit. Ihr Normskala ist:

Datum	Phishing Mails
August 14	943.407
September 14	1.632.682
Oktober 14	1.218.232
November 14	898.688
Dezember 14	1.211.293
Januar 15	1.228.161
Februar 15	660.670
März 15	1.920.309
April 15	1.286.725
Mai 15	983.008
Juni 15	691.404
Juli 15	824.108

Größten Drei
1.920.309
1.632.682
1.286.725

Durchschnitt
1.613.239

Normskala	Absolutwert	Normwert
0%	0	0
-10%	161.324	1
-20%	322.648	2
-30%	483.972	3
-40%	645.295	4
-50%	806.619	5
-60%	967.943	6
-70%	1.129.267	7
-80%	1.290.591	8
-90%	1.451.915	9
90% und mehr	1.613.239	10

Sie messen aktuell "755.432". Normalisiert ist das eine "5".

3. Index der Bedrohungslage

2. Den Indexwert berechnen (in %)

Die nächsten Schritte (Gewichtung, Score berechnen) sind identisch zum Verwundbarkeitsindex .

Interne Metriken	Aktuell	Vergleichswert	%	Normalisiert	Gewichtet	Normskala 0 1 2 3 4 5 6 7 8 9 10	
Metric 1	755.432	1.613.239	46,8%	5	1	X	10
Metric 2	133	173	77,0%	8	2	X	20
Metric 3	521	639	81,6%	9	1	X	10
Metric 4	145	178	81,6%	9	2	X	20
Metric 5	11	16	67,3%	7	3	X	30
Externe Metriken							
Cybersecurityindex.com	2.814	2.764	1,8%	2	1	X	10
				Score	**71**		100

$$Index\ der\ Bedrohungslage = \frac{71}{100} \cdot 100 = \mathbf{71}$$

4. Index der Gefährdungslage

$$Index\ der\ Gefährdungslage = \frac{Index\ der\ Verwundbarkeit + Index\ der\ Bedrohungslage}{2}$$

$$Index\ der\ Gefährdungslage = \frac{34{,}3 + 71}{2} = \mathbf{52,7}$$

Das können Sie natürlich auch anders machen!

34,3

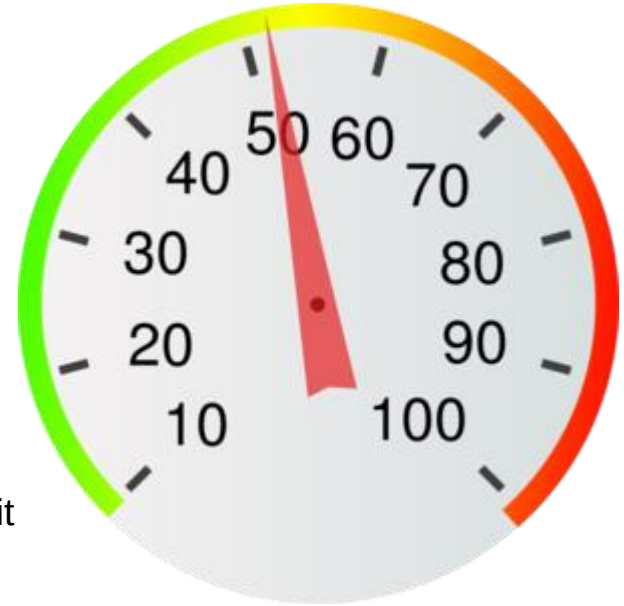
52,7

71

4. Index der Gefährdungslage

Gefährdung = Bedrohung + Verwundbarkeit

Hohe Verwundbarkeit / Wenig Bedrohungen
Geringe Verwundbarkeit / Viele Bedrohungen



Geringe Verwundbarkeit
Wenig Bedrohungen

Hohe Verwundbarkeit
Viele Bedrohungen

Das Modell ist …

- skalierbar von einer kleinen Organisation bis zu einem Konzern.
- basierend auf der Systematik des BSI.
- anpassbar an vorhandene Metriken.
- flexibel an den Reifegrad des Security-Managements anpassbar.
- verständlich, auch für Nicht-Fachleute.

Letzte Worte

- Der "Index der Gefährdungslage" auf einem Dashboard sollte nur ein Einstiegspunkt sein.
- Achtung: "Blinder Fleck"!
- Passen Sie das Modell an Ihre Bedürfnisse an!
- Nehmen Sie die Metriken, die Sie brauchen (und haben).
- Make it simple, but not too simple!
- Holen Sie sich Unterstützung aus der BI-Abteilung!
- Automatisieren Sie die Datenlieferungen.
- Verkleinern Sie die Berichtszyklen wo möglich.
- Definieren Sie realistische Normskalen.

Vielen Dank!

Holger Himmel (CISM, T.I.S.P.)
CISO, Tengelmann WHG KG, Mülheim an der Ruhr, Germany

hhimmel@uz.tengelmann.de
http://de.linkedin.com/in/holgerhimmel

Literatur

- H.Himmel, Index der Gefährdungslage, IT-Governance, Mai 2015, S. 17
- H.Himmel and A.Sowa, Ein Tacho für IT-Sicherheit, <kes> - Zeitschrift für Informations-Sicherheit, August 2015, S. 37

Credits
Picture of Albert Einstein: Photographer: Yousuf Karsh, archived by www.calie.org
Tachometer: www.clker.com