

Fallstudie: Die Heim PC Lösung

Jennifer Lodewyks & Fabian Gröger

28. März 2018

Inhaltsverzeichnis

1. Fallstudie: Die Heim PC Lösung	2
2. Risikoanalyse	3
<i>2.1. Risikogewichtung.....</i>	<i>6</i>
3. Massnahmenplan für ein Budget bis CHF 500.-	7
<i>3.1. Risikosituation nach den Massnahmen.....</i>	<i>8</i>
4. Fazit	9

1. Fallstudie: Die Heim PC Lösung

Die Familie Meier wohnt im 2. Stock eines 3-stöckigen Hauses mit 6 Wohnungen. Meiers haben 3 Kinder, Lilian (21), Jan (18) und Dora (12). Herr Meier hat eine verantwortungsvolle Position in der Schweizer Bundesverwaltung und macht 1-2 Mal pro Woche kleinere Arbeiten am Abend am PC. Frau Meier erledigt die finanziellen Angelegenheiten und die Buchführung der Familie.

Konfiguration:

Netzwerk besteht aus VDSL Zugriff (50 MBits/s)

1. Eltern PC = Server (Printer File und Media), feste 1 GBit Verdrahtung
2. 5 Smartphones, 2 Tablets, 2 Kameras und 10 Sensoren sind per WLAN angeschlossen.
3. 3 Kinder Laptops sind sowohl per Kable als auch per WLAN angeschlossen.
4. WLAN brauch WEP
5. Alle Computer brauchen MS OS die 2 Smartphone mit IOS und 3 mit Android.

Weiter Verwendungszwecke der Kinder: Snapchat, Twitter, Facebook, Onlinebanking, IP Telefonie, Skype und Web Browsing. Hausaufgaben vergleichen/lösen über E-Mails und FAX am PC.

Onkel Özutöck, der Schwager von Frau Meier, hilft Meiers den PC Installation fit zu halten. Er bringt manchmal Programme (oder Spiele) mit, welche er von seinem Laptop auf die PCs überspielt.

2. Risikoanalyse

Was könnte alles schiefgehen? Im folgenden Teil wird eine Risikoanalyse über den Fall von der Familie Meier gemacht, welche Probleme bei ihnen auftreten können und wie schwerwiegend diese wären.

Risikoquelle:	1. Hackerangriffe
Beschreibung:	Die Computer, Kameras, Sensoren und Smartphones könnten durch Hacker angegriffen werden, welche sich somit einen Zugang ins System der Familie Meier beschaffen. Sie bekommen die Kontrolle über Sensoren und Kamera, und somit Aufnahme oder Verbreitung von Bildmaterial (Verletzung der Privatsphäre). Beschaffung und Missbrauch von vertraulichen Daten auf den Computern und Smartphones der Familie.
Risikoeinstufung:	Eintrittswahrscheinlichkeit: selten Auswirkung: kritisch Vertretbarkeit: bedingt vertretbar Risikostufe: 5

Risikoquelle:	2. Fremde im System
Beschreibung:	Fremde, wie zum Beispiel der Onkel der Familie Meier könnten die privaten Daten oder die Daten der Firma, welche von den Eltern mit nach Hause genommen wurden, einsehen oder kopieren.
Risikoeinstufung:	Eintrittswahrscheinlichkeit: möglich Auswirkung: kritisch Vertretbarkeit: nicht vertretbar Risikostufe: 7

Risikoquelle:	3. Viren
Beschreibung:	Durch runterladen von unbekannten Dateien aus dem Internet durch Eltern oder auch von den Kindern.
Risikoeinstufung:	Eintrittswahrscheinlichkeit: möglich Auswirkung: kritisch Vertretbarkeit: nicht vertretbar Risikostufe: 7

Risikoquelle:	4. E-Mails/Phishing
Beschreibung:	Die Familie erhält Spam-E-mails, mit Links zu unseriösen Seiten, oder Dateien im Anhang mit Viren. Vor allem Gefährdung bei den Kindern, welche unbedacht sich solche E-Mails ansehen.
Risikoeinstufung:	Eintrittswahrscheinlichkeit: möglich Auswirkung: kritisch Vertretbarkeit: nicht vertretbar Risikostufe: 7

Risikoquelle:	5. Kinder
Beschreibung:	Ungenügende oder keine Verschlüsselung von vertraulichen Daten (z.B. Bankdaten) und somit kommen die Kinder zu diesen Informationen. Kinder kommen auf für sie ungeeignete Seiten wie z.B. Pornoseiten, wo sie u.a. auch Viren auf den Computer laden.
Risikoeinstufung:	Eintrittswahrscheinlichkeit: gelegentlich Auswirkung: gering Vertretbarkeit: bedingt vertretbar Risikostufe: 4

Risikoquelle:	6. Programme und Spiele von Freunden/Fremden
Beschreibung:	Die Familie bekommt von einem Onkel Programme und Spiele, haben aber unter Umständen keine Lizenzen. Die Spiele oder Programme könnten auch Viren enthalten.
Risikoeinstufung:	Eintrittswahrscheinlichkeit: möglich Auswirkung: spürbar Vertretbarkeit: nicht vertretbar Risikostufe: 6

Risikoquelle:	7. Social Media
Beschreibung:	Die Kinder sind bei Facebook, Twitter etc. angemeldet und können dort unkontrolliert von Fremden angesprochen und ausgehorcht werden. Sie bekommen viel Werbung und somit mögliche Virenübertragungen, wenn sie auf Videos und geteilte Sachen klicken.
Risikoeinstufung:	Eintrittswahrscheinlichkeit: möglich Auswirkung: spürbar Vertretbarkeit: nicht vertretbar Risikostufe: 6

Risikoquelle:	8. Datenverluste
Beschreibung:	Die Hardware könnte ausfallen durch Kurzschlüsse, veraltete Hardware, Unfälle (Wasser auf Geräte) oder Verlieren des Smartphones und somit ein Datenverlust entstehen.
Risikoeinstufung:	Eintrittswahrscheinlichkeit: selten Auswirkung: katastrophal Vertretbarkeit: nicht vertretbar Risikostufe: 6

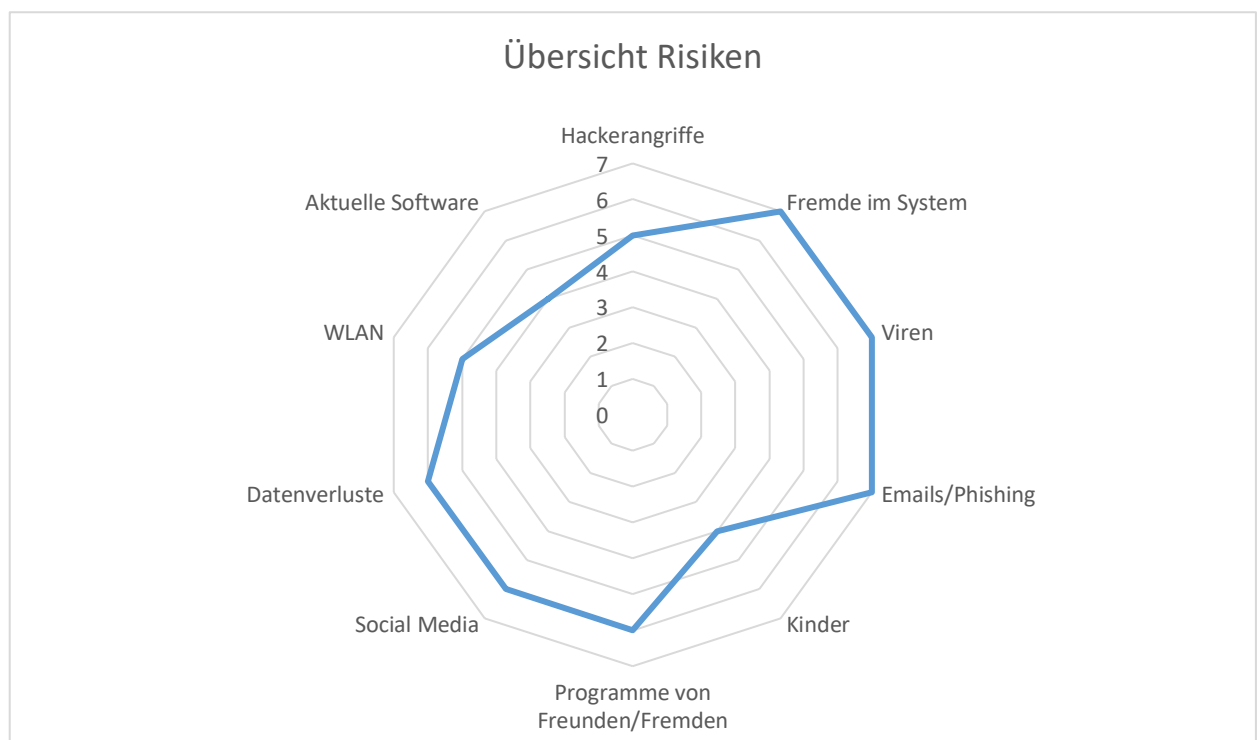
Risikoquelle:	9. WLAN
Beschreibung:	Wird das WLAN der Familie ausreichend mit Passwörtern und Verschlüsselung geschützt? Was ist mit den Smartphones, welche über das WLAN laufen?
Risikoeinstufung:	Eintrittswahrscheinlichkeit: selten Auswirkung: kritisch Vertretbarkeit: bedingt vertretbar Risikostufe: 5

Risikoquelle:	10. Aktuelle Software
Beschreibung:	Das Betriebssystem könnte nicht aktuell sein und neuste Updates sind nicht installiert, was Sicherheitslücken hervorrufen kann. Auch die Virenprogramme benötigen immer die aktuellsten Updates.
Risikoeinstufung:	Eintrittswahrscheinlichkeit: gelegentlich Auswirkung: gering Vertretbarkeit: bedingt vertretbar Risikostufe: 4

2.1. Risikogewichtung

Eintrittswahrscheinlichkeit	häufig	5	6	7	8	9
	möglich	4	5	6	7	8
	gelegentlich	3	4	5	6	7
	selten	2	3	4	5	6
	unwahrscheinlich	1	2	3	4	5
		unbedeutend	gering	spürbar	kritisch	katastrophal
Auswirkungen						

	Vor den Massnahmen:				
	Risiko	Eintrittsw.	Auswirkung	Vertretbarkeit	Risikostufe
1	Hackerangriffe	selten	kritisch	bedingt vertretbar	5
2	Fremde im System	möglich	kritisch	nicht vertretbar	7
3	Viren	möglich	kritisch	nicht vertretbar	7
4	Emails/Phishing	möglich	kritisch	nicht vertretbar	7
5	Kinder	gelegentlich	gering	bedingt vertretbar	4
6	Programme von Freunden/Fremden	möglich	spürbar	nicht vertretbar	6
7	Social Media	möglich	spürbar	nicht vertretbar	6
8	Datenverluste	selten	katastrophal	nicht vertretbar	6
9	WLAN	selten	kritisch	bedingt vertretbar	5
10	Aktuelle Software	gelegentlich	gering	bedingt vertretbar	4

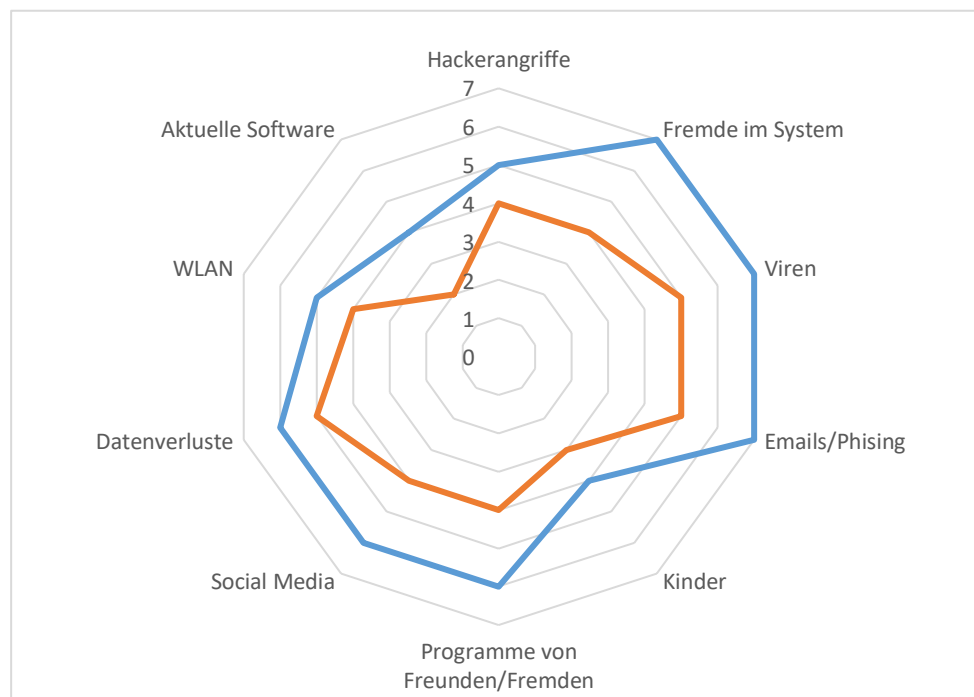


3. Massnahmenplan für ein Budget bis CHF 500.-

1. Die Risiken **1,2** und **9** können vermindert werden, wenn der Router von WEP durch ein WLAN-Router mit WPA2 ausgetauscht wird. Es wird ein schwer knackbares Passwort eingesetzt, das nur den Eltern bekannt ist, und dass sie bei allen Geräten selber eingeben müssen.
Kosten: ca. CHF 100.-
2. Risiko **6** kann vermindert werden, indem Onkel Özutöck durch eine entsprechende Schulung, lernt von wo man aktuelle Programme herunterlädt und wie man deren Integrität mittels des Hash-Wertes überprüft.
Kosten: ca. CHF 100.-
3. Risiko **8** kann vermindert werden, indem man eine einfache Backup-Lösung von Windows verwendet, und auf einer externen Festplatte die Datensicherung einrichtet.
Kosten: ca. CHF 50.-
4. Risiken **3, 4, 5** und **7** können vermindert werden, indem man ein gutes Antivirenprogramm korrekt installiert und tägliche kleinere und wöchentliche vollständige Scans festlegt. Damit heruntergeladener Schadcode und Viren erkannt und vernichtet werden.
Kosten: ca. CHF 100.-
5. Risiko **10** kann vermindert werden, indem Frau und Herr Meier entsprechend geschult werden, wie man einen Rechner aktuell und sicher hält. Ausserdem soll in dieser Schulung auch gezeigt werden, wie mit dem neu installierten Antivirenprogramm umzugehen ist und wie man sich zu verhalten hat wenn der Rechner infiziert ist. Ausserdem sollte in dieser Schulung noch kurz über einen bewussten Internetumgang gesprochen werden, der nach der Schulung den Kindern auch beigebracht werden soll.
Kosten: ca. CHF 150.-

3.1. Risikosituation nach den Massnahmen

	Nach den Massnahmen:				
	Risiko	Eintrittsw.	Auswirkung	Vertretbarkeit	Risikostufe
1	Hackerangriffe	unwahrscheinlich	kritisch	bedingt vertretbar	4
2	Fremde im System	unwahrscheinlich	kritisch	bedingt vertretbar	4
3	Viren	selten	kritisch	bedingt vertretbar	5
4	Emails/Phishing	selten	kritisch	bedingt vertretbar	5
5	Kinder	selten	gering	vertretbar	3
6	Programme von Freunden/Fremden	selten	spürbar	bedingt vertretbar	4
7	Sozial Media	selten	spürbar	bedingt vertretbar	4
8	Datenverluste	selten	spürbar	bedingt vertretbar	4
9	WLAN	unwahrscheinlich	kritisch	bedingt vertretbar	4
10	Aktuelle Software	unwahrscheinlich	gering	vertretbar	2



4. Fazit

Die grössten Sicherheitsrisiken in dieser Fallstudie gehen vor allem auf diese wichtigen Faktoren zurück:

- Einsatz veralteter Sicherheits-Technologie (WEP)
- Falsches, fahrlässiges Verhalten
 - Im Umgang mit dem Internetverhalten
 - Im Umgang mit Datensicherung
 - Im Umgang mit Aktualisierungen
- Kein Einsatz von Antivirenprogramm

Viele Risiken konnten durch das Ersetzen der WEP-Verschlüsselung durch eine aktuellere Technologie stark verkleinert werden, ohne dass dabei grosse Kosten entstanden sind.

Einige Risiken (Programme vom Onkel und aktuelle Software) konnten mittels Schulungen gemindert werden. Dies funktioniert aber nur, wenn das dort eingeübte Verhalten konsequent eingehalten wird.

Manche Massnahmen zielen darauf ab, die Menge der Schadensfälle bzw. deren Eintrittswahrscheinlichkeit zu minimieren, so etwa das Ersetzen von WEP durch WPA2. Andere Massnahmen helfen dabei, das Schadensausmass zu reduzieren, so das Durchführen einer regelmässigen Datensicherung.

Insgesamt konnten die Sicherheitsrisiken der Familie Müller mit nur CHF 500.-, stark verbessert werden. Wenn man noch mehr Geld investieren würde, könnte man die Risiken noch stärker verbessern, z.B. durch eine aktuelle und sichere Firewall und die Segmentierung des Heimnetzwerks in unterschiedliche Sicherheitszonen.