

Inhalt

Über den Autor	9
Einleitung: Alles wird zum Computer	11
Dank	27
TEIL I Die Schwachstellen	31
1 Computer sind immer noch schwierig zu sichern	35
Die meiste Software ist schlecht programmiert und unsicher	36
Sicherheit spielte bei der Entwicklung des Internets keine Rolle	38
Erweiterbarkeit heißt, alles kann gegen uns verwendet werden	41
Aufgrund ihrer Komplexität sind computerisierte Systeme einfacher anzugreifen als zu schützen	44
Interkonnektivität schafft neue Sicherheitslücken	46
Computer sind auf besondere Weise gefährdet	48
Die Angriffe werden immer besser, schneller und einfacher	51
2 Patches ist keine Lösung	55
Installation der Patches	58
Schreiben und Veröffentlichen der Patches	60
Offenlegen der Sicherheitslücken	63
Aufspüren der Sicherheitslücken	64
3 Internetnutzer zu identifizieren, wird immer schwieriger	67
Die Authentifizierung wird schwieriger, das Stehlen von Zugangsdaten einfacher	67
Die Attribution wird sowohl schwieriger als auch einfacher	76

4	Alle begünstigen Unsicherheit	81
	Das Internet wird immer noch durch den Überwachungskapitalismus gesteuert	82
	Im nächsten Schritt werden Unternehmen Kunden und User kontrollieren	85
	Auch Staaten nutzen das Internet zur Überwachung und Kontrolle	91
	Cyberkrieg wird zur Normalität	95
	Kriminelle profitieren von Unsicherheit	103
5	Die Risiken nehmen katastrophale Ausmaße an	109
	Die Angriffe auf die Datenintegrität und die Verfügbarkeit nehmen zu	109
	Algorithmen werden autonom und immer leistungsfähiger	113
	Unsere Lieferketten sind zunehmend angreifbar	119
	Es wird nur noch schlimmer	122
TEIL II Die Lösungen		131
6	Wie ein sicheres Internet+ aussehen könnte	137
	Absicherung der Geräte	140
	Absicherung der Daten	142
	Absicherung der Algorithmen	144
	Absicherung der Netzwerkverbindungen	146
	Absicherung des Internets	147
	Absicherung kritischer Infrastruktur	149
	Systeme voneinander trennen	152
7	Wie wir das Internet+ absichern können	155
	Standards entwickeln	157
	Fehlgerichtete Anreize korrigieren	160
	Haftungsfragen klären	166
	Informationsasymmetrie ausgleichen	172
	Öffentliche Aufklärung verbessern	178

	Berufliche Standards einführen	179
	Dem Fachkräftemangel begegnen	181
	Forschung weiter ausbauen	182
	Wartung und Instandhaltung fördern	183
8	Der Staat ermöglicht Sicherheit	185
	Eine neue Regierungsbehörde	186
	Staatliche Regulierung	192
	Herausforderungen der Regulierung.	194
	Normen, Verträge und internationale Aufsichtsbehörden.	199
9	Wie der Staat die Defensive der Offensive vorziehen kann.	205
	Offenlegen und Beheben von Sicherheitslücken	207
	Design zugunsten der Sicherheit, nicht der Überwachung.	213
	So viel wie möglich verschlüsseln	217
	Sicherheit und Spionage voneinander trennen.	219
	Strafverfolgung verbessern	221
	Die Beziehung zwischen Regierung und Wirtschaft überdenken	224
10	Plan B: Was wahrscheinlich passieren wird	229
	Die USA werden so schnell nichts unternehmen.	230
	Andere Länder werden regulieren	234
	Was wir tun können	238
11	Welche Fehler die Politik begehen kann	243
	Hintertüren fordern.	244
	Verschlüsselung beschränken	249
	Anonymität verbieten	251
	Massenüberwachung.	253
	Hacking Back	256
	Die Verfügbarkeit von Software begrenzen.	258

12 Für ein vertrauenswürdiges, resilientes und friedliches Internet+	261
Ein resilientes Internet	265
Ein entmilitarisiertes Internet	267
Résumé: Technologie und Politik zusammenbringen.	271
Ergänzende Hinweise und weiterführende Informationen	281
Stichwortverzeichnis	377