secorvo
security consulting

Secorvo Security News

Juni 2015

Von Medizinern lernen

Dass eine gesetzliche Immunität nicht vor Trojanerangriffen schützt mussten jüngst auch die Abgeordneten des Deutschen Bundestages schmerzlich erfahren. Und sie sind in guter Gesellschaft: Die Zahl der Fälle, in denen Angreifer über gut gemachte E-Mail-Anhänge und unveröffentlichte Sicherheitslücken (Zero-Day-Attacken) in Unternehmen eindringen, nehmen nachweislich zu.

Dabei sind die bekannten Fälle möglicherweise nur die Spitze eines (großen) Eisbergs: Wie im Bundestag bleiben die Angriffe häufig lange unentdeckt. Denn komplexe Angriffssoftware kümmert sich auch um den eigenen Schutz: Mit herkömmlichen Tools ist sie meist nicht aufzuspüren, und wenn die Aktivitäten des Trojaners unterhalb der Wahrnehmungsschwelle des Benutzers bleiben, schöpft dieser auch keinen Verdacht.

Gegen Angriffe dieser Art ist unser etabliertes Instrumentarium – ein Sicherheitskonzept plus präventive Schutzsysteme – schnell mit seinem Latein am Ende. Da hilft auch kein ‚fingerpointing' auf das Risiko vor dem Bildschirm – denn bei einem sorgfältig vorbereiteten, gezielten Angriff ist ‚Aufpassen' keine adäquate Schutzmethode. Wenn schon der Virenscanner die Schadsoftware nicht erkennen kann, wie soll dies dann dem Anwender glücken?

Vielleicht müssen wir angesichts dieser Herausforderungen den Beruf des Informations-Sicherheitsbeauftragten neu denken. Denn es geht uns inzwischen ähnlich wie den Medizinern: Auch wenn wir die Zusammenhänge immer besser verstehen, werden Krankheiten komplexer, Therapien spezialisierter, entwickeln Viren Resistenzen gegen bislang wirksame Medikamente und suchen sich neue Infektionswege. Neue Medikamente haben wiederum unbekannte Nebenwirkungen – damit steigt die Unübersichtlichkeit. Mediziner haben darauf mit Diversifizierung und Spezialisierung reagiert. Dabei haben sie gegenüber uns Technikern einen uneinholbaren Vorteil: Ihre Patienten heilen meist von selbst. Auch trotz der Therapie.

Inhalt

secorvo
security consulting

Security News

Der Chirurg

Der unvermeidliche ‚Trade-off' zwischen erzielbarer Sicherheit und Benutzerakzeptanz kann gelegentlich den Chirurgen erfordern. Denn manchmal geht es nicht ohne operativen Eingriff.

So benötigen Trojaner einen Kommunikationsweg, um von einem Endsystem aus mit dem Angreifer zu kommunizieren. Schneidet man das Unternehmensnetz in mehrere Teilnetze, so kann man die externe und interne Kommunikation entkoppeln. Das Surfen im Internet lässt sich beispielsweise über einen Terminalserver mit Browser realisieren, während das Endsystem nur auf das interne Netz zugreifen kann. Hat der Browser eine Malware eingefangen, kann diese nicht auf interne Daten zugreifen. Der Download von Daten aus dem Internet funktioniert dann allerdings nicht mehr ganz so bequem über einen Quarantänebereich.

Der Internist

Die aktuellen Infektionswege zwingen zu einer genaueren Beschäftigung mit den inneren Organen. So können durch eine Separierung von Anwendungen deren Daten vor anderen, möglicherweise infizierten ‚Organen' geschützt werden. Technisch realisierbar ist so etwas über Virtualisierungslösungen wie Qubes OS oder Docker. Dabei läuft jede Anwendung in einem eigenen Kontext, damit bei einem Sicherheitsproblem nur die jeweilige virtuelle Plattform betroffen ist, nicht aber das Gesamtsystem oder weitere Anwendungen. Der Datenaustausch zwischen diesen Plattformen sollte restriktiv gehandhabt werden.

Leider ist dieser hochinteressante Ansatz ab Werk bisher nur für eine Handvoll Anwendungen wie Firefox, Thunderbird und Libreoffice verfügbar. Für eigene Anwendungen muss ggf. eine Windows-VM etabliert werden.

Der Infektionsschutz kann durch die Innere Medizin erheblich gesteigert werden. Risiken und Nebenwirkungen sollten jedoch mit den betroffenen Benutzern abgestimmt werden.

Der Psychologe

Der Psychologe kümmert sich um den Menschen, darum, was dieser denkt und fühlt. Ihn interessieren weniger technische Lösungen sondern Maßnahmen, die auf das Verhalten der Menschen zielen. Er greift da ein, wo es in ungesunder Weise von der gesetzten Norm abweicht.

Eines seiner Instrumente ist die Durchführung wirksamer Awareness-Kampagnen, die mit Wahrnehmungs- und Verhaltensgewohnheiten brechen und einprägsam wesentliche Kernbotschaften vermitteln. Statistiken und Messungen helfen ihm, den Erfolg seiner Maßnahmen zu überprüfen.

Der Labordiagnostiker

Die Labordiagnostik untersucht Proben auf Befunde und versucht, aus den Ergebnissen zusammen mit der Bewertung anderer Symptome eine Diagnose zu erstellen. Auch in der Informationssicherheit sollte man die Diagnose nicht allein auf Symptome wie Anzeichen für Schwächen oder Berichte über Vorfälle stützen. Ein Labordiagnostiker solle regelmäßig Proben analysieren, um Infektionsgefahren frühzeitig zu erkennen. Die Ergebnisse von Schwachstellenscans und Penetrationstest können Handlungsbedarf aufzeigen.

Wie in der Medizin sind auch hier Erfahrung und die richtigen Werkzeuge der Schlüssel zur zutreffenden Diagnose. Konkrete Ansätze findet man z. B. bei PCI, beim BSI, beim NIST sowie im OWASP OTG und OWASP ASVS.

Der Notarzt

Gelegentlich sind akut lebensrettende Maßnahmen für die Versorgung eines Notfallpatienten erforderlich. Treten eine Störung des Bewusstseins, der Atmung, des Kreislaufes oder Lähmungen, Verbrennungen, Vergiftungen, Schuss-, Stich- oder Hiebverletzungen lebenswichtiger Organe auf, sollte spätestens 10 bis 15 Minuten nach Eingang des Notrufs der Notarzt seinen Einsatzort erreichen. Kommt er zu spät, können auch Fachwissen und Reanimation dem Notfallpatienten meist nicht mehr helfen.

Zwar ist auch der Notarzt der Informationstechnik gelegentlich von einem Fehlalarm betroffen. Oft aber stößt er auf zunächst unerklärliche Effekte auf der Ebene der Betriebssysteme oder im Netzwerkverkehr, die Symptome einer getarnten Schadsoftware sein können.

Die Auswertung von zusammengeführten Logdaten und Netflows bringt ihn, manchmal mit Unterstützung des »*Labodiagnostikers* oder, wenn er zu spät gekommen ist, des »*Pathologen*, auf die Spur des Krankheitsbilds und erlaubt ihm eine Einschätzung, wie kritisch der Grad der Verletzung bzw. der Infektion für das einzelne System und die gesamte Infrastruktur ist. Wird er zu spät gerufen, lassen sich betroffene Infrastrukturbereiche nicht mehr isolieren und es bleibt ihm nur, der IT eine Totenbescheinigung auszustellen.

secorvo
security consulting

Der Anästhesist

Der Anästhesist sorgt dafür, dass die Vitalfunktionen des Patienten während operativer und diagnostischer Eingriffe aufrechterhalten werden. Ein medizinischer Eingriff ist eine Krise – und der Anästhesist ihr Manager. Egal ob sich ein Hackerangriff, ein Systemausfall oder eine sonstige Krise im Unternehmen ereignet: es bedarf eines Krisenmanagers, der den Überblick und den Puls des Unternehmens im Auge behält, der mit allen Beteiligten in Kontakt steht und sie bei Bedarf beruhigt. Das gilt gleichermaßen für interne Beteiligte wie für interessierte Dritte, etwa die Presse.

Vor allem aber muss er den Patienten im Blick behalten, damit der Eingriff, die Säuberung der IT-Systeme und der Tausch von Hard- und Software, trotz des Zeitdrucks in geordneten Bahnen verläuft.

Der Anästhesist muss sich in vielen Disziplinen wenigstens grundsätzlich auskennen, er muss Situationen einschätzen, entscheiden und moderieren können. Vor allem aber muss er für Ruhe und Gelassenheit sorgen, damit der Patient die Operation gut übersteht.

Der Pathologe

Auch nach einer erfolgreichen (Not-) Operation gibt es noch offene Fragen. Wie konnte es dazu kommen? Was waren die Ursachen? Wie lässt sich so etwas in Zukunft vermeiden?

Der Pathologe unterstützt die Bewertung und Behandlung von Notfällen und Infektionen durch die Analyse von Gewebeproben (Biopsie) und Obduktionen. Er untersucht sowohl funktionierende IT-Systeme, bei denen Auffälligkeiten festgestellt wurden, als auch Systeme, die ohne erkennbaren Grund ihre Funktionen eingestellt haben.

Dabei gewinnt er Metadaten aus Hauptspeicherabzügen und Festplattenduplikationen und wertet diese zielgerichtet aus. Kann er die Infektion eines Systems feststellen, veranlasst er Quarantänemaßnahmen zur Eingrenzung der Ansteckungsgefahr. Sollte es zu einem Abfluss von Vitaldaten gekommen sein, werden die Nachweise so dokumentiert, dass sie im Streitfall gerichtsverwertbar sind.

Das Gesundheitsamt

Die Gesundheitsämter wachen über Hygiene und Epidemien. Eine wesentliche Säule sind Meldepflichten, die auch in der IT-Sicherheit langsam Einzug in Gesetze halten. Beispiele sind § 109a TKG, § 42a BDSG, § 15a TMG oder § 83a SGB X. Hinzu kommt die Einführung von Meldepflichten in dem vor der Verabschiedung stehenden IT-Sicherheitsgesetz: § 8b Abs. 4 BSIG-E wird künftig die Betreiber kritischer Infrastrukturen zur Meldung verpflichten.

Empfänger der Meldungen sind die Datenschutzaufsichtsbehörden, die Bundesnetzagentur und künftig das Bundesamt für Sicherheit in der Informationstechnik (BSI). Ähnlich den Datenschutzaufsichtsbehörden kann auch das BSI bald Auflagen zur Beseitigung von Sicherheitsmängeln erteilen.

Damit entsteht eine staatliche, auf Informationssicherheit bezogene Aufsicht. Im Gesundheitswesen wurde mit den Gesundheitsämtern der Grundstein für eine erfolgreiche Epidemiebekämpfung gelegt.

Secorvo News

Secorvo ist ‚Top Consultant'

Am vergangenen Freitag, den 26.06.2015, wurde Secorvo in Essen als eines der besten deutschen Beratungsunternehmen für den Mittelstand ausgezeichnet. Das Urteil der Jury ist das Ergebnis einer Bewertung der Professionalität von Secorvo in elf Dimensionen durch zehn mittelständischen Referenzkunden, die wissenschaftlich ausgewertet wurde. Die Auszeichnung überreichte Bundespräsident a. D. Christian Wulff.

Wer ‚Java' sagt, sollte auch sichere Softwareentwicklung meinen.

Die Sicherheit von Java-Webanwendungen hatte lange Zeit einen guten Ruf. Tatsächlich ist Java jedoch nicht sicherer oder unsicherer als andere Programmiersprachen. Spätestens mit den zahlreichen Java-Sicherheitsproblemen der vergangenen Jahre hat sich diese Erkenntnis herumgesprochen. Auf dem nächsten KA-IT-Si-Event am **16.07.2015** stellt Dominik Schadow (BridgingIT) in seinem Vortrag Sichere Webanwendungen mit Java typische Fallstricke bei der Planung, Entwicklung und Wartung von Java-Webanwendungen vor und zeigt, wie man diesen wirkungsvoll in allen Phasen eines Entwicklungsprojekts zu Leibe rücken kann (zur Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juli 2015	
16.07.	Wer 'Java' sagt, sollte auch sichere Softwareentwicklung meinen. (KA-IT-Si, Karlsruhe)
August 2015	
01.-06.08.	Blackhat USA 2015 (Blackhat, Las Vegas/US)
06.-09.08.	DEFCON 23 (DEFCON, Las Vegas/US)
09.-13.08.	15th Annual DFRWS Conference 2015 (DFRWS, Philadelphia/US)
12.-14.08.	24th USENIX Security Symposium (Usenix, Washington D.C./US)
16.-20.08.	Crypto 2015 (IACR, Santa Barbara/US)
31.08.	Sommerakademie (ULD, Kiel)
September 2015	
08.-09.09.	D•A•CH Security (Gemeinsame Arbeitskonferenz GI OCG BITKOM SI TeleTrusT, Sankt Augustin)
15.-17.09.	Future Security 2015 (Fraunhofer VVS, Berlin)
17.09.	Informationstag "Elektronische Signatur" 2015 (TeleTrust, Berlin)
21.-25.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Fundsache

Wer schon immer wissen wollte wie Gedankenlesen funktioniert - im folgenden 2,5minütigen Video wird dieses Mysterium aufgelöst.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Michael Knopp, Christoph Schäfer, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de