Computerviren - eine lästige Sache

Autor(en): **Weiersmüller, René**

Objekttyp: **Article**

Zeitschrift: **Schweizer Ingenieur und Architekt**

Band (Jahr): **107 (1989)**

Heft 4

PDF erstellt am: **07.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-77034

durch festgelegte und aufgrund der Versagenswahrscheinlichkeit abgeleitete Bemessungwerte konkretisiert. Die Begriffe wie Versagenswahrscheinlichkeit, Sicherheitsbedingung, Gefährdungsbilder, menschliches Versagen, akzeptiertes Risiko und Sicherheitsplan (vgl. auch Glossar, Seite 68) fanden bereits ihren Eingang im Normenwerk.

Es war nicht leicht, den traditionellen Weg zu verlassen und das neue Sicherheitsdenken durchzusetzen. Es wurden dementsprechend auch Kompromisse getroffen. Es ist deshalb nicht erstaunlich, dass der Einzug des neuen Sicherheitsdenkens in das Normenwerk viele Jahre in Anspruch nahm. Der nächste Schritt – die Umsetzung in die Praxis – steht erst bevor.

Durch die Festlegung der sicherheitsrelevanten Sachverhalte in Sicherheitsplänen werden die Gefahren und die zu deren Reduktion vorgesehenen Massnahmen sowie die eingegangenen Risiken ersichtlich. Die Sicherheit wird auf die eliminierten Gefahren bezogen und der Sicherheitsbegriff dadurch konkretisiert. Die Sicherheitsplanung stellt demnach eine neue Aufgabe und damit eine neue Herausforderung an die Ingenieure dar.

Adresse des Verfassers: Dr. sc. techn. *M. Matousek*, Abt. Sicherheit, Qualitätssicherung, UVP; Wenaweser + Wolfensberger AG, Ingenieure + Architekten, Reinhardstrasse 10, 8034 Zürich.

Computerviren – eine lästige Sache

Als Computerviren werden kleine Manipulationsprogramme bezeichnet, die – einmal in den Computer eingeschleust – zu Systemabstürzen, Datenveränderungen oder unerwünschten Programmabläufen führen können. Trotz weitestgehender Absicherung können die Folgen – vor allem bei untereinander vernetzten Computersystemen – katastrophal sein.

Im folgenden wird neben einigen allgemeinen Erläuterungen ausführlich ein spezifisches Virusproblem auf einem zwar weniger im kommerziellen Sektor eingesetzten, aber doch weit verbreiteten Computer – dem Amiga von Commodore – beschrieben.

Weder eine opportunistische Herunterspielung der Virenprobleme noch Panikmache ist hier am Platz, hat sich

VON RENÉ WEIERSMÜLLER, SCHLIEREN

doch schon manche Meldung über das Auftreten eines neuen Virus nachträglich als Angeberei oder als Folge eines Bedienungs-, Hardware- oder Softwarefehlers herausgestellt. Immerhin muss man sich im klaren sein, dass die absichtliche Verbreitung eines Computervirus einen kriminellen Akt darstellt, der mit Strafverfolgung (inkl. horrenden Schadenersatzforderungen) geahndet werden kann. Und einen absoluten Schutz vor Viren wird es selbst bei Grossanlagen nie geben!

Grundsätzlich ist jeder Computer – unabhängig von der Art des Betriebssystems – durch Viren ansteckbar. Die Verbreitung der Viren erfolgt im *Home- und Personalcomputer-Bereich* über Programm- und Datenaustausch (meist Disketten, zunehmend Mailboxen). Massgebend für Umfang und Häufigkeit einer Virusepidemie dürfte somit vor allem die Verbreitung eines Computersystems sowie der Umfang des Programmangebotes sein, bestimmen doch diese Faktoren, wie oft dieselben Disketten bzw. Programme auf mehr als nur einem Computer eingesetzt werden (legales oder illegales Kopieren, Austausch von Disketten, Programmvorführungen auf anderen Anlagen, Austesten von Fremdprogrammen usw.).

Einer der ersten Computerviren, die einen grösseren Bekanntheitsgrad erreichten, war der *SCA-Virus*. Bösartiger und vor allem weiter verbreitet scheint jedoch der *Byte-Bandit-Virus* zu sein, obschon dieser als Folge der typischen Symptome und dem Fehlen einer «Inkubationszeit» (unüberschaubare Verbreitung bis zur Entdeckung!) relativ einfach zu diagnostizieren ist. Das Schreckgespenst selbst für Grossanlagen soll z.Zt. ein Virus sein, der über das (nachträglich infizierte) Spielprogramm *Larry* in die Computer eingeschleust wird.

Der Byte-Bandit-Virus auf dem Amiga

Der Byte-Bandit setzt sich, wie die meisten der besonders verbreitungsfreudigen Viren, im Bootblock von Disketten fest. Massgebend für die Infizierung des Computers ist daher der *erste Lesezugriff* auf das Laufwerk *nach dem Einschalten des Computers* (nicht nach Reset!!): Ist diese erste Diskette (oder dementsprechend die Harddisk) mit dem Byte-Bandit verseucht, so wird der Computer unweigerlich angesteckt. Das schlimme dabei ist, dass nun jede weitere Diskette, die ohne Schreibschutz in das Laufwerk eingelegt wird, ebenfalls angesteckt wird und so eine lawinenartige Verbreitung des Fehlers auslösen kann.

Diese erste Diskette kann theoretisch auch eine nur formatierte, virusbefallene Leerdiskette sein. Meist wird es sich jedoch um eine Systemstartdiskette handeln. Ist hingegen diese ominöse erste Diskette als Systemstartdiskette frei vom Byte-Bandit, so kann der Computer durch nachfolgende, virusverseuchte Disketten nicht mehr angesteckt werden. D.h. «sauber» aufgestartet sind mit virusverseuchten Disketten weder Computer noch weitere Disketten ansteckbar.

Folgen des Virusbefalls

Der Byte-Bandit will sich vermehren. Das kann er aber nur, wenn Disketten ohne Schreibschutz in das Laufwerk des *infizierten Computers* gesteckt werden. Wird die Virusübertragung vom angesteckten Computer auf die Diskette durch den Schreibschutz verunmöglicht, erscheint meist sofort mit dem Einschieben der *schreibgeschützten Diskette* die Fehlermeldung «Error validating; Disk is unreadable». Dieses typische Symptom ist unabhänig davon, ob der *infizierte Computer* mit einer sauberen oder einer virusbefallenen Diskette «gefüttert» wird. Der Effekt tritt auch auf, wenn die schreibgeschützte Sy-

Einige allgemeine Vorsichtsmassnahmen gegen Virusbefall:

Disketten mit Originalprogrammen von Anfang an unbeschreibbar machen durch mechanisches Entfernen des Schreibschutz-Schiebers oder fixieren mit etwas Leim.

Beim Wechsel auf andere Programme Computer zuerst ausschalten. Besonders wichtig ist das nach dem Arbeiten mit fremden Disketten bzw. Programmen.

Beim Arbeiten (oder Spielen) mit fremden Disketten keine eigenen Disketten ins Laufwerk stecken, ohne den Computer vorher auszuschalten. Harddisk beim Arbeiten mit fremden Disketten ausgeschaltet lassen. Bei grossem Schadenpotential den Einsatz nicht systemzugehöriger Disketten grundsätzlich unterlassen.

So weit wie möglich mit schreibgeschützten Disketten arbeiten. Bisher ist noch kein Virus bekannt, der eine schreibgeschützte Diskette anstecken kann. Von wichtigen Daten zusätzlich von Zeit zu Zeit Sicherungskopien für längerfristige Archivierung erstellen.

Den Personenkreis, welcher Zugriff zum Computer hat, auf das Minimum beschränken.

stemstartdiskette, mit welcher der Computer angesteckt wurde, kurz aus dem Laufwerk genommen und wieder eingesteckt wird.

Gleichzeitig mit dem Erscheinen der Fehlermeldung startet das Laufwerk zu einem Dauerlauf. Nach dem Anklicken von «Cancel» kommt die Meldung «Disk struktur corrupt; Use Diskdoctor to correct it» und erst nach erneutem Anklicken von «Cancel» unterbricht die Floppy ihren Dauerlauf.

Je nach Programmstand bzw. Software erscheint nun auf dem Bildschirm

- das Diskicon Df0:NDOS, oder
- die Meldung «Not a Dosdisk in unit 0» (beim Anklicken von «Cancel» beginnt das Spiel von neuem), oder
- wird hartnäckig nach der bereits im Laufwerk vorhandenen Diskette verlangt, oder
- kann mit dem Programm weiter gearbeitet werden.

Letzteres ist auch der Fall, wenn von der vorher nicht akzeptierten Diskette der Schreibschutz entfernt wird (mit Sicherheit ist die Diskette jedoch anschliessend vom Byte-Bandit befallen).

Da meist mit Disketten ohne Schreibschutz gearbeitet wird, sind die obengenannten Symptome häufig nicht erkennbar. Folgende Fehloperationen wurden in diesem Fall bei Befall durch den Byte-Bandit bisher beobachtet:

- reproduzierbar keine Formatierung mehr möglich,
- unregelmässig auftretende Mausstörungen (Kontaktprobleme und «Hänger»),
- unregelmässig auftretende Bildausfälle (Bildschirm wird dunkel oder nimmt die Farbe der Workbench an),
- wahrscheinlich Verstellen der batteriegepufferten Uhr in der Speichererweiterung.

Herkunft des Byte-Bandit-Virus

Unbekannt. Es ist nicht einmal mit Sicherheit ausschliessbar, dass der Virus über Fehlbedienung und/oder ein Hard- bzw. Softwarefehler selbst zu erzeugen ist. Wenn dem so wäre, müsste allerdings offen bleiben, ob der Byte-Bandit noch als Virus im eigentlichen Sinne zu bezeichnen wäre.

Abtöten des Virus

Mit Reset kann der Virus nicht aus dem *Computer* vertrieben werden; jener bleibt so immer noch aktiv. Virusfrei wird der Computer hingegen durch genügend langes Ausschalten (mind. zehn Sekunden).

Mit dem Diskdoctor (auf der Workbench) ist der Virus auf der *Diskette* nicht zu entfernen. Das Formatieren der verseuchten Diskette (geht wie erwähnt nur mit virusfreiem Computer) zerstört zwar den Virus, jedoch auch den Disketteninhalt. Wird dieser noch gebraucht (was meist der Fall sein wird), muss der Virus anders abgetötet werden. Bereits fehlerhafte Datensätze oder Programme können so allerdings nicht wieder hergestellt werden. Das können auch die *käuflichen Viruskiller-Programme* nicht, die zudem meist spezifisch auf die Eliminierung eines bestimmten Virus ausgelegt sind.

Wie erwähnt nistet sich der Byte-Bandit auf dem Bootblock der Diskette ein. Mit dem Install-Befehl kann dieser neu überschrieben werden. Sofern noch eine virusfreie Workbench vorhanden ist, empfiehlt sich z.B. folgendes Vorgehen: Computer zuerst durch Ausschalten (mind. zehn Sekunden) vom Virus befreien. Dann *saubere Workbench* laden und über CLI

1› MAKEDIR RAM:C

1› COPY SYS:C TO RAM:C

1› ASSIGN C: RAM:C

eingeben (jede Zeile mit RETURN abschliessen). Nun kann es losgehen mit der Entseuchung: Virusbefallene Diskette ohne Schreibschutz ins Laufwerk, INSTALL DFO: eingeben und mit RETURN abschliessen, Diskette raus, nächste rein, INSTALL DFO: usw. Achtung: In Einzelfällen entspricht der Bootblock nicht dem Standardeintrag mit dem Install-Befehl. In solchen Fällen müsste der Bootblock nach dem Überschreiben wieder angepasst werden. Einfacher dürfte es dann sein, wenn mit virusfreiem Computer vom Originalprogramm eine Kopie gemacht und diese auf den aktuellen Stand gebracht wird durch Kopieren der *Daten oder Programmänderungen* von der virushaltigen Diskette.

Ist keine saubere Workbench mehr da, aber eine beliebige, virusfreie Systemstart-Diskette mit dem CLI und dem Befehl ASSIGN, so kann die Workbench z.B. so geheilt werden: Computer mind. zehn Sekunden ausschalten, dann die saubere Startdiskette laden, CLI aufrufen und ASSIGN C: (NAME DER VERSEUCHTEN WORKBENCH): C eingeben und mit RETURN abschliessen. Der Name der verseuchten Workbench (ohne Klammern eingeben) muss dabei aus einem Wort bestehen (evtl. zuerst umbenennen!). Nachdem der Computer nach der verseuchten Diskette verlangt hat, kann INSTALL DFO: eingetippt werden und die Diskette ist virusfrei.

Ausblick

Bis jetzt hat der Verfasser dieser Zeilen in dieses Virusproblem so viel Zeit investiert, wie nötig wäre, um seine Briefe, Buchhaltungsarbeiten und Manuskripte der nächsten Jahre von Hand zu erstellen. Glauben Sie deshalb nicht, durch den Computer würden Arbeitsplätze gespart. Das Gegenteil ist der Fall – wenn sich auch die Art der Tätigkeit etwas ändern wird. Selbst von dem auch für den Mann von der Strasse erschwinglichen, superschnellen 64-Bit-Computer mit einem Gigabyte Speicherkapazität in Schuhschachtelgrösse (Zukunftsmusik) wird diesbezüglich keine Gefahr ausgehen. Engpässe sehe ich eher darin, wenn unser menschlicher Geist hard- und softwaremässig mit dem Niveau und den exponentiell zunehmenden Tücken solcher Superapparate nicht mehr ganz mithalten kann.

Adresse des Verfassers: *René Weiersmüller*, Dipl. Chemiker HTL/SIA, Industriestr. 11, 8952 Schlieren.