COMPUTER-VIREN: EVOLUTION, EIGENSCHAFTEN, SCHUTZ

Осипов Д.И., Юруть Н.Г.
Научный руководитель: ст. преподаватель Пужель Т.В.
Белорусский национальный технический университет

In der Informationsgesellschaft stellen Computer-Viren eine ernsthafte Bedrohung dar, die eine sorgfältige Untersuchung erfordert. Diese schädlichen Programme, die auf Computersysteme abzielen, werden immer komplexer und wecken ein erhöhtes Interesse im Bereich der Cybersicherheit.

Im Bericht werden die Erforschung der Evolution von Computer-Viren, die Identifizierung ihrer Merkmale und die Analyse von Schutzmethoden vorgestellt. Von ihren ersten Erscheinungen bis zu ihren modernen Formen stellen Viren ernsthafte Risiken für Privatpersonen, Unternehmen und Regierungen dar.

Die Bedeutung des Verständnisses der Gründe für die Erstellung von Viren und der Motivation ihrer Autoren ist unbestreitbar. Wir bemühen uns, die Folgen von Virusangriffen aufzudecken, wie z.B. den Verlust vertraulicher Informationen und finanzielle Verluste. Das Ziel ist es, Empfehlungen für die Sicherheit in der digitalen Umgebung zu entwickeln und die Strategien zur Bekämpfung von Computer-Viren zu verbessern.

Computer-Viren sind schädliche Programme, die in Computersysteme eindringen und ihnen Schaden zufügen können. Computer-Viren können nach verschiedenen Kriterien klassifiziert werden, wie z.B. nach dem Typ, dem Infektionsweg und der Verstecktechnik.

Gefahr von Computerviren. Computer-Viren stellen eine ernsthafte Bedrohung für die Sicherheit und das Funktionieren von digitalen Systemen sowie für die Vertraulichkeit und Integrität von Daten dar. Sie können verschiedene Arten von Schäden verursachen, wie z.B.:

1.*Verlust oder Beschädigung von Daten.* Viren können Dateien auf dem Computer löschen, verändern oder verschlüsseln, so dass sie für einen Benutzer unzugänglich oder nutzlos werden. Es gibt ein Beispiel: der Virus WannaCry hat Dateien auf Computern verschlüsselt und Lösegeld für ihre Wiederherstellung gefordert.

2. *Leistungseinbußen.* Viren können den Computer verlangsamen, indem sie Ressourcen des Prozessors, des Speichers oder der Festplatte verbrauchen. Zum Beispiel, der Virus Stuxnet hat bis zu 50% der Prozessorzeit genutzt, um seine Aktivität zu verbergen.

3. *Sicherheitsverletzung.* Viren können Lücken in der Sicherheit des Computers öffnen, die es Angreifern ermöglichen, auf das System oder das Netzwerk zuzugreifen. Ein Beispiel dazu: der Virus Conficker hat ein Botnetz aus infizierten Computern erstellt, das für Angriffe auf andere Ziele genutzt werden konnte.

4. *Informationsdiebstahl.* Viren können persönliche oder vertrauliche Daten eines Benutzers abfangen, kopieren oder senden, wie z.B. Passwörter, Bankdaten, Kontakte, Dokumente usw. Zum Beispiel, der Virus Zeus hat sich auf den Diebstahl von Daten für das Online-Banking spezialisiert.

Evolution. Computerviren sind ein einzigartiges Phänomen in der Welt der Informationstechnologie. Schauen wir uns ihre Geschichte an und überlegen wir, wie sie sich seit ihrer Einführung entwickelt hat.

Die Theorie der sich selbst reproduzierenden Automaten: In den späten 1940er Jahren diskutierte der Mathematiker John von Neuman zum ersten Mal die Idee von Computerviren. Er stellte ein Gedankenexperiment vor, das die Möglichkeit eines „mechanischen" Organismus untersucht – Computercode, der eine Maschine beschädigen kann, indem er Kopien von sich selbst erstellt und die Maschine infiziert, ähnlich wie ein biologisches Virus.

Creeper-Programm: Im Jahr 1971 schuf BBN-Mitarbeiter Bob Thomas das Creeper-Programm, das zum ersten Virus wurde. Es wurde als Testprogramm entwickelt, um die Fähigkeit zur Selbstreplikation zu testen. Der Creeper hat neue Festplatten infiziert und versucht, Daten vom vorherigen Computer zu löschen.

Rabbit-Virus: Das bösartige Rabbit-Virus (oder Wabbit) wurde 1974 erstellt. Es hat sich selbst reproduziert, die Systemleistung beeinträchtigt und das Abstürzen des Computers dadurch verursacht.

Erster Trojaner: Im Jahr 1975 schuf der Programmierer John Walker den ersten ANIMAL-Trojaner. Es war ein Programm, das andere Malware in sich verbarg.

Im Laufe der Zeit wurden Viren komplexer und vielfältiger. Sie stellen immer noch eine Bedrohung für die Sicherheit von Computern dar, und ihre Bekämpfung bleibt für Antivirenprogramme und Sicherheitsexperten eine wichtige Aufgabe.

Nach dem Typ werden Computer-Viren unterteilt in:

Netzwerk-Viren verbreiten sich über Computernetzwerke, indem sie Datenübertragungsprotokolle, E-Mails, Dateiaustausch usw. nutzen. Die Beispiele für Netzwerk-Viren sind: Melissa, ILOVEYOU, Mydoom1.

Datei-Viren infizieren ausführbare Dateien und Programme, indem sie ihren Code hinzufügen. Die Beispiele für Datei-Viren sind: Jerusalem, Parity Boot, CIH2.

Boot-Viren infizieren die Boot-Sektoren von Datenträgern, die den Code zum Starten des Betriebssystems enthalten. Die Beispiele für Boot-Viren sind: Brain, Stoned, Michelangelo3.

Datei-Boot-Viren kombinieren die Eigenschaften von Datei- und Boot-Viren, indem sie sowohl Dateien als auch Boot-Sektoren infizieren. Die Beispiele für Datei-Boot-Viren sind: One Half, Form, Yankee Doodle4.

Nach dem Infektionsweg werden solche Computer-Viren unterschieden:

Residente Viren bleiben im Arbeitsspeicher des Computers nach der Infektion und fangen Zugriffe auf Dateien oder Datenträger ab, um sie zu infizieren. Die Beispiele für residente Viren sind: Randex, CMOS, Meve.

Nicht-residente Viren bleiben nicht im Speicher und sind nur während der Infektion aktiv. Die Beispiele für nicht-residente Viren sind: Cascade, Vienna, Trivial.

Nach der Verstecktechnik werden Computer-Viren unterteilt in:

Replikative Viren kopieren ihren Code in andere Dateien oder Sektoren, ohne deren Größe oder Inhalt zu ändern. Die Beispiele für replikative Viren sind: Elk Cloner, Creeper, Ping-Pong.

Trojanische Programme tarnen sich als nützliche oder harmlose Programme, führen aber schädliche Aktionen aus. Die Beispiele für trojanische Programme sind: Back Orifice, SubSeven, Netbus.

Logische Bomben werden unter bestimmten Bedingungen aktiviert, z.B. nach Datum, Zeit, Ereignis usw. Die Beispiele für logische Bomben sind: Friday the 13th, Chernobyl, AIDS.

Mutanten ändern ihren Code bei jeder Infektion, um die Erkennung und Entfernung zu erschweren. Die Beispiele für Mutanten sind: MtE, Dark Avenger, Phoenix.

Unsichtbare verbergen ihre Präsenz im System durch verschiedene Methoden, wie das Abfangen von Datei- oder Festplattenanforderungen, das Verschlüsseln des Codes usw. Unsichtbare Beispiele sind Stealth, Frodo, Wal.

Makro-Viren infizieren Makros, die Sets von Befehlen zur Automatisierung von Aktionen in Anwendungen sind, z.B. in Texteditoren oder Tabellen. Die Beispiele für Makro-Viren sind: Concept, Melissa, Wazzu.

Schutz vor Computerviren. Um sich vor Computer-Viren zu schützen, muss man folgende Maßnahmen ergreifen:

1. *Installation und Aktualisierung von Antiviren-Software.* Antiviren-Programme können Viren erkennen und entfernen sowie vor verdächtigen Dateien oder Links warnen. Zum Beispiel kann man Kaspersky Internet Security verwenden, um den Computer zu schützen.

2. *Einhaltung der Regeln der Hygiene im Internet.* Öffnet man keine verdächtigen Anhänge oder Links in E-Mails, lädt man keine Dateien aus unbekannten Quellen herunter. Man muss keine unsicheren Websites besuchen, keine gleichen oder schwachen Passwörter verwenden, sich nicht mit unsicheren Wi-Fi-Netzwerken verbinden usw.

3. *Datensicherung.* Man muss Kopien der wichtigen Dateien auf externen Medien oder in Cloud-Diensten speichern, damit man sie im Falle einer Virusinfektion wiederherstellen kann. Man kann, zum Beispiel, Kaspersky Backup verwenden, um Backups der Daten zu erstellen.

Also, Viren sind Malware. Sie können verschiedene Funktionen ausführen, die meisten sind jedoch negativ. Dieses Thema ist heutzutage sehr relevant. Der Informationsfortschritt steht nicht still. Der weltweite Einfluss von Computern nimmt zu, und leider verschärft sich auch das Problem von Computerviren immer mehr. Und das ist normal. Davon kann man nirgendwohin kommen. Man muss einfach die Sicherheitsregeln im Netzwerk beachten.

Литература

1. Классификация компьютерных вирусов [Электронный ресурс]. – Режим доступа : https://bitdefender.ua/ru/blog/klassifikatsiya-kompyuternyh-virusov/. – Дата доступа : 27.02.2024.

2. Computervirus [Elektronische Ressource]. – Das Regime des Zugriffes : https://www.hornetsecurity.com/de/wissensdatenbank/computervirus/. – Das Datum des Zugriffes : 01.03.2024.

3. Computerviren – Geschichte und Ausblick [Elektronische Ressource]. – Das Regime des Zugriffes : https://www.kaspersky.de/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds. – Das Datum des Zugriffes : 01.03.2024.

NEUE RICHTUNGEN DER LOGISTIKENTWICKLUNG IN DER REPUBLIK BELARUS

Перхурович М.А.
Научный руководитель: ст. преподаватель Пужель Т.В.
Белорусский национальный технический университет

Die Republik Belarus ist ein kontinentales Land. Sie ist ein Binnenstaat und hat nur wenige natürliche Ressourcen. Aber die günstige Lage des Landes ist von besonderer Bedeutung für den Transit und die Suche nach neuen vielversprechenden Märkten für Verkehrsdienste.

Das Territorium von Belarus wird von zwei transeuropäischen Verkehrskorridoren durchquert: West-Ost und Nord-Süd.

Die Autobahn Brest – Minsk – die Russische Föderation ist ein Abschnitt des transeuropäischen Verkehrskorridors II: Berlin – Warschau – Minsk – Moskau – Nishni Nowgorod. Der Korridor verbindet vier Länder: Deutschland, Polen, Belarus und Russland. Dieser Verkehrskorridor ist wichtig, da er Ost und West miteinander verbindet.

Seit 2020 haben die EU und die USA jedoch Sanktionen gegen Belarus verhängt. Dies führte zu Schwierigkeiten für die moderne Logistik des Landes. Der