Der Morris-Computerwurm oder „The same procedure as every year"

Kommentar von Michael Veit, Cybersecurity-Experte bei Sophos

Wie zu Beginn jedes Jahres stehen auch 2023 wieder unzählige Prognosen zur Verfügung, in welche Richtung sich die Cybercrime-Landschaft entwickeln wird. Allerdings ist der Blick in die Glaskugel – auch wenn noch so viele Indizien zur Verfügung stehen – immer nur eine Wette auf die Zukunft. Interessanter ist deshalb einmal ein Blick auf die Ursachen der Cyberattacken im Lauf der Geschichte. Und hier wird schnell deutlich, dass wir im Prinzip seit mehreren Jahrzehnten immer wieder über die gleichen drei Tigerfellköpfe stolpern.

Unser historischer Bezug geht auf den 2. November 1988 zurück, den Tag, an dem ein dramatischer Internet-Wurm seinen Anfang nahm. Die nach dem Informatiker Robert T. Morris benannte Schadsoftware breitete sich vor über 30 Jahren alarmierend schnell aus und gilt als die erste große Malware-Attacke. Der Morris-Wurm verfügte über drei primäre Selbstreplikationsmechanismen, die auf drei häufigen Programmier- und Systemverwaltungsfehlern beruhten:

1. **Speicher-Missmanagement:** Morris nutzte eine Pufferüberlauf-Schwachstelle in einem damals beliebten Systemnetzwerkdienst aus und erreichte RCE (Remote Code Execution).
2. **Schlechte Passwortwahl:** Morris nutzte einen sogenannten Dictionary-Angriff, um wahrscheinliche Login-Passwörter zu erraten. Er musste nicht jedes Passwort erraten – es reichte aus, nur ein einziges zu knacken.
3. **Ungepatchte Systeme:** Morris suchte nach E-Mail-Servern, die unsicher eingerichtet, aber später nie aktualisiert wurden, um die gefährliche Remote-Code-Ausführungslücke zu beheben, die er missbraucht hatte.

Klingt bekannt? Sollte es, denn auch im vergangenen Jahr haben wir heruntergebrochen kollektiv weiterhin unter der gleichen Art von Cybersicherheitsproblemen gelitten und werden auch 2023 mit diesen „Tigerfellköpfen" zu tun haben. Es heißt also grundsätzlich auch in diesem Jahr „The same procedure as every year" – wir benötigen keine Unmengen neuer Vorhersagen zur Cybersicherheit, um eine wirklich gute Vorstellung davon zu haben, wo wir anfangen sollen.

Der Blick zurück nach vorn

Mit anderen Worten: Wir dürfen bei der Erstellung von Cybersecurity-Konzepten die Grundlagen nicht aus den Augen verlieren und sollten es vermeiden, nur bestimmte und aktuell schlagzeilenträchtige Sicherheitsprobleme zu lösen. Nur wenn wir die Cybersicherheitssünden der Vergangenheit in den Griff bekommen, können wir auch effektiv gegen moderne Cyberbedrohungen vorgehen.

Was ist also zu tun? Die gute Nachricht ist, dass Hersteller in Sachen Programmierung immer besser darin werden, mit vielen dieser Probleme der alten Schule umzugehen. Zum Beispiel lernen wir, sicherere Programmierpraktiken und sicherere Programmiersprachen zu verwenden und unseren laufenden Code in Sandboxes mit besserer Verhaltensblockierung einzubetten, um das Ausnutzen von Pufferüberläufen zu erschweren.

Wir lernen alle immer besser, Passwort-Manager zu nutzen, obwohl sie ihre eigenen faszinierenden Probleme mit sich bringen. Wir sind immer geübter darin, alternative Technologien zur Identitätsprüfung anzuwenden oder verlassen uns nicht auf simple Passwörter, von denen wir hoffen, dass sie niemand vorhersagen oder erraten wird. Noch besser ist aber Multifaktor-Authentifizierung, die wir überall nutzen sollten, wo es möglich ist.

Und wir bekommen nicht nur Patches schneller von Anbietern (zumindest verantwortungsbewussten – der Witz, dass das S in IoT für Security steht, scheint leider immer noch sehr aktuell zu sein), sondern zeigen uns sowohl im privaten als auch geschäftlichen Umfeld zunehmend bereit, Patches und Updates schneller einzuspielen.

Gut Ding bekommt Weile

Wir bei Sophos, ebenso wie andere in der Branche, setzen uns zudem stark für moderne CaaS-Technologien (Cybersecurity as a Service) wie XDR und MDR ein, was bedeutet, dass wir akzeptieren, dass es beim Umgang mit Cyberangriffen nicht nur darum geht, Malware zu finden und bei Bedarf zu entfernen. Heutzutage neigen wir viel mehr als noch vor ein paar Jahren dazu, Zeit zu investieren, um nicht nur nach bekanntermaßen schlechten Sachen Ausschau zu halten, die behoben werden müssen, sondern auch dafür zu sorgen, dass die guten Sachen, die dort sein sollen, tatsächlich vorhanden sind, und sie auch wirklich etwas Nützliches tun.

Wir nehmen uns auch mehr Zeit, um proaktiv nach potenziell schädlichen Dingen zu suchen, anstatt zu warten, bis die sprichwörtlichen Warnungen automatisch in unseren Cybersicherheits-Dashboards erscheinen. Und das sind die besten Voraussetzungen, um Cyberkriminelle auch 2023 in ihre Schranken zu weisen – und elegant über den Tigerfellkopf zu hüpfen.

Social Media von Sophos für die Presse

Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de