Computeria

www.computeria-wallisellen.ch

IT-Sicherheit

Markus Deller

Heutige Themen

- Kurzer Rückblick auf letzte Präsentation
- PC Schutzfunktionen verstehen
- Datenschutz in Windows 10
- Spectre und Meltdown

Rückblick

- Onlinekonten und Absicherung
- Virenscanner, dafür und dagegen
- Werbeblocker
- Datensicherung

Security

- „Schaden kann es nicht“
- „Besser als gar nichts“
- „Je mehr desto besser“

„Schaden kann es nicht“

Beispiel Firewall von früher:

- Zugang wurde abgeriegelt, nur ausgewählte Programme hatten Zugang zum Internet
- Trojaner schafften es trotzdem auf den PC
- Andere Dienste funktionierten z.T. nicht mehr (Bsp. Auto-Update)

„Schaden kann es nicht“

Beispiel Auto-Update- Mechanismus:

- Wurde zum Teil bei Programmen abgeschaltet
- Dadurch mögliche Infizierung wegen veralteter und unsicherer Programme
- Im Extremfall keine Antivirus-Updates mehr
- → führt also zu weniger statt mehr Sicherheit

„Besser als gar nichts“

- Veraltete Verschlüsselungsverfahren sind angreifbar
- Wurden auf Server häufig als ‚Fallback‘ für veraltete Client-Software verwendet
- Sind (viel schneller) zu knacken, also primärer Angriffspunkt
- Betrafen 2016 ca. einen Drittel aller HTTPS-Webserver

Beispiel: HTTPS-Webserver

„Besser als gar nichts“

- Veraltete Verschlüsselung wurde erzwungen und mit wenig Aufwand geknackt
- Zentrales Geheimnis des Servers wurde errechnet, das alle Verbindungen schützt
- Eigentlich sichere Verbindungen konnten abgegriffen werden
- Daten konnten im Nachhinein auch von sicheren Verbindungen entschlüsselt werden
- → veraltete Verschlüsselung ist hier also nicht besser als gar keine, sondern eine akute Gefahr

„Je mehr desto besser“

Beispiel eines realen Falls einer Firma:

- Für eine Präsentation im Konferenzraum fehlte eine wichtige Datei
- Wegen Sicherheit konnten keine USB-Sticks verwendet werden (Steckplätze versiegelt)
- Kein gemeinsames Netz für Dateiaustausch vorhanden
- Datei konnte nicht beschafft werden und Präsentation drohte zu platzen

„Je mehr desto besser“

„Lösung“ des Beispiels:

- Datei wurde über privates E-Mail geschickt
- Präsentator rief Mail im Raum über Web-Mail ab
- → Die sensible Datei wurde hier also unverschlüsselt übers Internet verschickt und lag dann auf einem nahezu ungeschützten Mail-Server!

Schädlingsabwehren

- Firewall
- Sicherheitsupdates
- Virenschutz
- Noscript, Adblock

Firewall

- Filtert Verkehr ins und aus dem Internet
- Auf PC „personal Firewall“
- Auf Netzwerkebene (Router) „klassische Firewall“

Firewall schützt:

- Vor unerwünschten Zugriffen auf lokale Dienste, z.B. bei Nutzung eines öffentlichen Hotspots

Firewall schützt nicht:

- Vor Abfluss persönlicher Daten
- Vor Infektion durch Viren

Firewall, zu beachten:

- Firewalls können den Ablauf von Programmen beeinflussen oder stören
- Fehlkonfigurationen verhindern im Heimnetz Dienste (z.B. Drucken und Freigaben)

Sicherheitsupdates

- Sicherheitslücken in Hard- und Software werden geschlossen
- z. T. Neue Schutzfunktionen
- Wichtigste Komponenten: Betriebssystem, Browser, Office, Router

Sicherheitsupdate schützt:

- Vor Angriffen, bei denen Lücken ausgenutzt werden (z.B. beim Öffnen einer Word-Datei)

Sicherheitsupdate schützt nicht:

- Vor Infektion mit Schadcode, die der Benutzer selbst ausführt (bewusst oder unbewusst)
- Vor Zero-Day-Lücken, die im Geheimen ausgenutzt werden, bevor Updates existieren

Sicherheitsupdate zu beachten:

- Hastig veröffentlichte Updates können System oder Programme lahmlegen, wenn nicht genügend getestet (Bsp. Januar-Patch Windows)

Virenschutzprogramme

- Machen Jagd auf Schädlinge aller Art und
- Verhindern dessen Ausführung
- Versuchen, ein verseuchtes System zu desinfizieren
- Überwachen das Verhalten mittels Muster

Antivirus schützt:

- Vor Infektion durch bekannte Schädlinge
- Häufig vor unbekannten Viren, die durch Verhalten auffallen
- Vor unabsichtlicher Weitergabe von Schadcode

Antivirus schützt nicht:

- Vor der Ausnutzung von Sicherheitslücken
- Vor ganz frischen Schädlingen, die noch nicht in den Antivirusdatenbanken enthalten sind

Antivirus, zu beachten:

- Nachrüstbare Programme kosten Geld und/oder zeigen Werbung
- Fehlalarme sind möglich
- Es wird häufig ‚nach Hause telefoniert‘
- Windows 10 bringt von Haus aus einen Schutz mit (Defender)

Adblocker

- Sehr beliebt, da häufig Webseiten ohne die Werbedaten schneller geladen werden
- Haben positiven Einfluss auf Privatsphäre und Sicherheit
- Bringen Webseitenbetreiber um ihre Einnahmen

Adblocker schützt:

- Vor Tracking durch Werbung
- Vor Schadcode, der über Anzeigenetzwerke ausgeliefert wird

Adblocker schützt nicht:

- Vor Angriffscode, der direkt in die Website eingebettet wurde

Skriptblocker

- Verhindert Ausführung von aktiven Inhalten (Javascript, Flash)
- Kann (und wird) die meisten Seiten erstmal falsch bzw. unvollständig anzeigen
- Benötigt vor allem zu Beginn manuelle Anpassungen

Skriptblocker schützt:

- Vor Angriffen, die Sicherheitslücken ausnutzen
- Vor Tracking
- Vor XSS-Angriffen (Cross-Site-Scripting)
- Vor Clickjacking

Skriptblocker schützt nicht:

- Vor Download von Viren
- Vor Angriffen, bei denen eine ‚erlaubte‘ Site kompromittiert wurde
- Vor Phishing

Blocker, zu beachten:

- Teilweise werden Adblocker von der Site erkannt und sperren Nutzer aus
  → meist Abschalten erforderlich
- Betreiber werden um ihre Werbeeinnahmen gebracht
- Bei Skriptblock funktionieren Websites häufig zuerst mal nicht
- Häufig Eingreifen des Benutzers notwendig (Feintuning)

Überwachter Ordnerzugriff

- In Windows 10 mit Fall Creators Update eingeführt
- Schränkt den Zugriff auf Ordner ein für bestimmte Programme

Ordnerüberwachung schützt:

- Vor Verschlüsselung durch Krypto-Trojaner
- Vor unerlaubter Manipulation wichtiger Dateien durch nicht autorisierte Prozesse

Ordnerüberwachung schützt nicht:

- Vor der eigentlichen Infektion durch Malware
- Vor Abgreifen vertraulicher Informationen

Vorhandene Schutzfunktionen

- Virenschutz, Firewall, der Sicherheitsupdate-Mechanismus und überwachte Ordnerzugriff sind alle im neuesten Windows 10 enthalten
- Ad- und Skriptblocker sind als Erweiterungen oder z.T. schon eingebaut im Browser zu finden, allerdings ohne Feineinstellungs- möglichkeit

Vorhandene Schutzfunktionen

Wir sind also momentan geschützt vor:

- Unerwünschten Zugriffen aus dem Netz
- Veraltetem System
- Infektion durch und Weitergabe von Schädlingen
- Teilweise vor Tracking (Ausspionieren) und Schadcode beim Surfen

Sich im Netz bewegen

- Transportverschlüsselung
- Privates Browsen

Transportverschlüsselung

- Mail und Web können Verkehr verschlüsseln
- Verkehr zwischen Server und PC kann von Dritten abgehört werden
- Daten selbst sind auf dem Server meist unverschlüsselt gelagert

Transportverschlüsselung schützt:

- Vor Massenüberwachung im Internet
- Mitlesen des Netzwerkverkehrs (Browsen und Mail) durch Dritte

Transportverschlüsselung schützt nicht:

- Vor gezielten, auf einzelne Personen gerichtete Überwachungsmassnahmen
- Vor Spionage

Transportverschlüsselung, zu beachten:

- Kann trügerische Sicherheit vorgaukeln
- HTTPS sagt nichts über die Vertrauenswürdigkeit des Anbieters aus

Privates Browsen

Benennung in einzelnen Browsern:

- Firefox, Safari, Opera: „privates Fenster“
- Chrome: „Inkognito-Fenster“
- Edge: „InPrivate-Fenster“

Privates Browsen

- Im privaten Modus wird der Browser keine Daten speichern, die Aufschluss über die besuchten Seiten geben.
- Nach Beenden des Browsers werden alle Daten der Sitzung gelöscht: besuchte Seiten, Cookies, Suchabfragen, temporäre Dateien

Privates Browsen schützt:

- Vor anderen Nutzern des Browsers. Man kann verbergen, welche Seiten man angesurft hat. Dies ist insbesondere bei öffentlichen Computern sinnvoll.
- (Interessante Seiten sollte man als Lesezeichen speichern, sie sind sonst nach der Sitzung verschwunden)

Privates Browsen schützt nicht:

- Vor Verfolgung im Internet. Es werden nur angefallene Spuren gelöscht, eine Anonymisierung findet nicht statt.
- Vor Downloads oder Lesezeichen (die bleiben erhalten)

Weitere Schutzmassnahmen

- Backup
- Verschlüsselung auf PC
- UAC

Backup

- Jedes Backup ist besser als kein Backup!
- Ideal ist die 3-2-1-Regel: 3 Kopien auf mindestens 2 verschiedenen Medien, 1 davon ausser Haus.

Backup schützt:

- Vor Datenverlust durch Fehlbedienung, Krypto-Trojaneren, Hardwaredefekten.
- Vor Datenverlust durch Diebstahl, Elementarschäden (wenn min. 1 Backup extern gelagert)

Backup schützt nicht:

- **Wenn man es nicht macht!**
- Dies tönt banal, ist aber der häufigste Grund, warum Daten nicht wiederhergestellt werden können
- Wenn es nur 1 Medium gibt und dies genau dann von Trojanern befallen wird, während es angeschlossen ist.
- Datenklau

Verschlüsselung

- Verschiedene Arten existieren, Dateiebene, Container- oder Laufwerkverschlüsselung
- Schlüssel- oder Passwortverlust bedeutet Datenverlust

Verschlüsselung schützt:

- Den Inhalt von Dateien, auch beim Kopieren auf andere Laufwerke

Verschlüsselung schützt nicht:

- Die Datei selbst. Sie kann also kopiert, verändert oder gelöscht werden.
- Vor weiterer Verschlüsselung durch Krypto-Trojaner

Benutzerkontosteuerung (UAC)

- UAC schützt vor ungewollten Änderungen am System
- Administrator hat nicht automatisch volle Rechte, die müssen erst bestätigt werden
- Ist nicht vollständig wasserdicht, es gibt Techniken zur Umgehung der Abfrage

UAC schützt:

- Die Windows-Komponenten und einen Grossteil der installierten Software vor Manipulationen durch Schädlinge

UAC schützt nicht:

- Vor Trojanern, Viren und Malware, die ohne besondere Rechte laufen können
(zum Verschlüsseln der eigenen Dateien sind keine Admin-Rechte erforderlich)
- Vor Malware, welche die UAC-Abfrage mit Tricks umgehen kann
- Wenn man sie bedenkenlos bestätigt

Zusammenfassung

- Vor allem die weiteren Schutzfunktionen benötigen ein gewisses Mass an Aufwand für den Benutzer.
- Die gezeigten Funktionen dienen primär zur Ausfallssicherheit und Privathaltung der Dateien

Spectre und Meltdown

- Beides sind Hardware-Sicherheitslücken in Mikroprozessoren
- Sie sind also auf den allermeisten PCs (und Macs) heute vorhanden
- Es sind z.T. auch Tablets und Smartphones davon betroffen
- AMD-Prozessoren sind von Meltdown derzeit nicht betroffen

Wirkungsweise

- Prozesse können über unauthorisierte Zugriffe Speicherinhalte von fremden Prozessen auslesen
- Ein Angriff kann so im Extremfall den gesamten physikalischen Speicher eines Systems auslesen
- Das Abgreifen von Informationen benötigt eine genaue Zeitmessung

Gegenmassnahmen

Da die Lücke vor allem über Webbrowser mittels schädlichem Javascript-Code ausgenutzt werden könnte, reagierten die Browserhersteller mit Programmaktualisierungen.

- Im Fall von Spectre können auch mit dem Einsatz von Skript- und Werbeblockern in Browsern aktive Inhalte verhindert oder eingeschränkt werden.

Gegenmassnahmen

Die Meltdown-Lücke wurde bei Windows mit den Januar-Updates behoben.

Um die Spectre-Lücke zu stopfen, ist ein Mikrocode-Aktualisierung erforderlich. Intel und AMD kündigten an, solche Updates zu veröffentlichen.

Die Lösungen müssen aber von den Computer- und Hardwareherstellern implementiert werden.

Gegenmassnahmen

Ältere Prozessoren oder Systeme erhalten eher keine Aktualisierungen mehr. Hier muss folglich ein Austausch der Hardware in Betracht gezogen werden.

Fazit

- Die beiden Lücken sind einerseits sehr gravierend, da sie wegen der Hardware auf nahzu allen heutigen Systemen vorhanden sind.
- Beide Lücken benötigen eine genaue Zeitauflösung, deshalb kann durch Herabsetzen derselben ein Angriff wirksam abgeschwächt werden
- Die Lösungen kosten Rechenleistung, dies kann sich deutlich spürbar in der Performance eines Systems zeigen.

Wir brauchen euch

- Bitte schickt uns Beispiele von Themen, die euch speziell beschäftigen.
- Vor allem in der Rubrik Alltägliche Probleme sind wir auch auf euren Input angewiesen.

direktes Mail an Markus Deller

??? Fragen ???

Vielen Dank fürs Zuhören