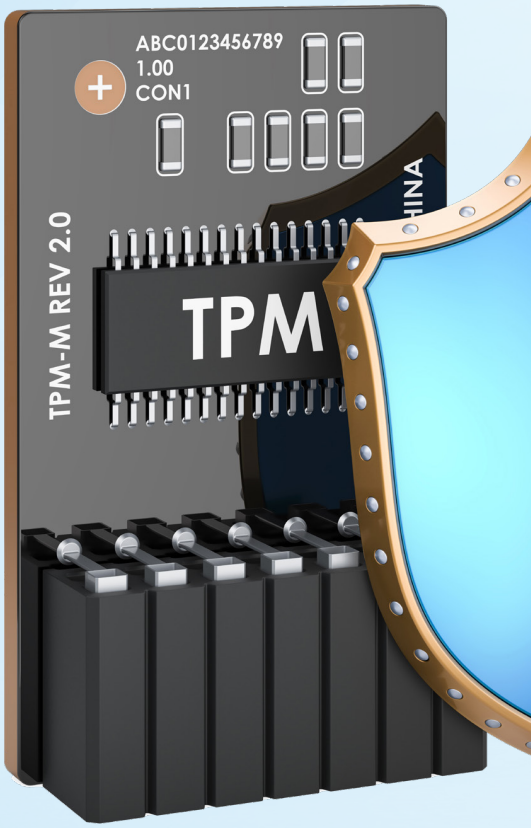
Windows 11

SCHRECK-GESPENST TPM?



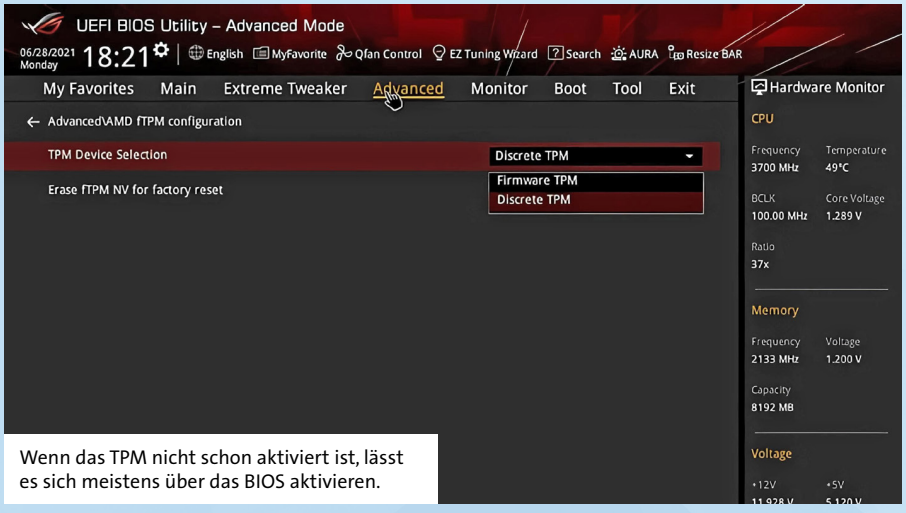
Das Sicherheitsmodul TPM ist einigen Datenschützern schon lange ein Dorn im Auge. Nun ist es eine Voraussetzung für Windows 11 und wird weiter für Diskussionen sorgen. Von Martin Dietrich

Windows 11 ist seit Anfang Oktober offiziell erhältlich und wird sich aller Voraussicht nach in den nächsten Monaten sukzessive auf dem PC-Markt ausbreiten. Um Microsofts neuestes Software-Flaggschiff installieren zu können, verlangt das Unternehmen zwingend das Sicherheitsmodul TPM 2.0. In vielen Fällen lässt sich die Technologie über das BIOS des Mainboards einschalten, wenn sie nicht schon aktiviert ist. Rechner, die älter als sechs Jahre sind, müssen allerdings womöglich nachrüsten, da ihnen die entsprechende Hardware fehlt.

Der Tech-Gigant begründet den Zwang mit erhöhter Plattformintegrität und mit dem Schutz vor Manipulationsversuchen. TPM 2.0 ist laut Microsoft ein »Grundpfeiler« der Windows-Sicherheit. In der Vergangenheit wurde jedoch schon heftig um TPM gestritten, weil Datenschützer potenzielle Hintertüren für Geheimdienste witterten und vor einer Entmündigung des Kunden warnten. 2013 kam es sogar zu einem kleinen Skandal, als Zeit Online berichtete, dass IT-Experten des Bundes Sicherheitsbedenken bezüglich Windows 8 und TPM 2.0 äußerten, die beide damals neu eingeführt wurden. Im Anschluss wehrte sich Microsoft erfolgreich vor Gericht gegen den Artikel und erwirkte eine Anpassung des Textes.

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) meldete sich im Zuge der damaligen Kontroverse und betonte, dass es die Öffentlichkeit keinesfalls vor einem Einsatz von Windows 8 warne. In bestimmten »Einsatzszenarien« gebe es jedoch einige kritische Aspekte im Zusammenhang mit TPM 2.0 zu beachten.

Wir haben bei zwei Kryptografieexperten und beim Bundesamt für Sicherheit in der Informationstechnik nachgefragt, wie sie die Sicherheit von TPM im Lichte der Veröffentlichung von Windows 11 einschätzen und ob die damaligen Bedenken heute noch zutreffen. Es äußern sich zum einen Dr. Stefan Köpsell von der Technischen Universität Dresden und zum anderen Prof. Dr. Rüdiger Weis von der Berliner Hochschule für Technik.



Wenn das TPM nicht schon aktiviert ist, lässt es sich meistens über das BIOS aktivieren.

Was ist TPM überhaupt und welchen Nutzen hat es?

TPM steht für Trusted Platform Module und ist eigentlich ein alter Hut. Schon Anfang der 2000er-Jahre gründeten Unternehmen wie Microsoft, Intel und HP die Trusted Computing Group. Gemeinsam konzipierten sie einen Chip, der im Zusammenspiel mit dem Betriebssystem sicherstellen soll, dass sich das gesamte System in einem vom Hersteller definierten, erwartbaren Zustand befindet und damit verschlüsselte Daten verschlüsselt bleiben. »TPM ist typischerweise ein spezielles Hardware-Sicherheitsmodul, das in Rechnern und Servern verbaut ist, indem kryptografische Schlüssel sicher hinterlegt werden können«, erklärt Dr. Köpsell. Die Art und Weise, wie Chip und Betriebssystem miteinander kommunizieren, beruht auf einem standardisierten Verfahren.

Die Implementierung des TPM auf Basis des Standards kann sich je nach Hardware-Produzent unterscheiden. Neben dem physischen Modul ist TPM nämlich mittlerweile auch als Firmware verfügbar (fTPM), die im Prozessor oder Chipsatz integriert sein kann. Bei Manipulationsversuchen am BIOS oder am Bootvorgang soll das TPM schnell Alarm schlagen. Zudem kann sich Microsoft aus der Ferne über den Zustand des Rechners informieren und theoretisch bestimmen, welche Programme darauf installiert werden dürfen. Kritiker vergleichen TPM deswegen auch gerne mit einem DRM-Verfahren, weil die Hersteller dadurch im Prin-

Warzone nutzt in Zukunft das Anti-Cheat-Programm Ricochet. Anstelle einer eigenen Software könnte TPM das übernehmen und das System theoretisch entlasten.

zip das Sagen haben, wie wir unsere PCs nutzen und modifizieren können.

Zwar sorgt die Technologie dafür, dass Angriffe auf das System registriert werden, selbst eingreifen kann es jedoch nicht. »TPM macht nur Sinn, wenn man ein prinzipiell sicheres System eigentlich schon hat«, sagt Köpsell. »TPM allein bringt gar nichts.« Man kann es sich ein bisschen so vorstellen wie bei einem zahnlosen Wachhund. TPM bellt laut, wenn es einen Einbrecher sieht, kann dem Dieb aber nicht in die Wade beißen.

Wie sicher ist TPM?

Eine hundertprozentige Sicherheit vor Angriffen kann es nicht geben, daran ändert auch TPM nichts. Inwieweit es der Sicherheit signifikant zugutekommt, ist allerdings unter Kryptografieexperten strittig.

»Wenn man sich anschaut, wie oft es Sicherheits-Updates von Browsern, dem Betriebssystem und der Anti-Viren-Software gibt, dann kann man schon die Frage stellen, ob nur, wenn sich das System in einem bekannten Zustand befindet, das dann wirklich bedeutet, dass dieser Zustand als sicher angesehen werden kann«, gibt Köpsell zu bedenken. Insgesamt entspreche TPM aber den derzeitigen Sicherheitsvorgaben, meint er. »Ich würde schon sagen, dass aktuell die ganze Geschichte als recht sicher angesehen werden kann.«

Im Gegensatz zur Vorgängerversion wurde bei TPM 2.0 beispielsweise die Festplattenverschlüsselung durch BitLocker verbessert. Dadurch, dass Windows 11 die aktuelle Version voraussetzt, kommt jeder in den Genuss der besseren Verschlüsselung.

Prof. Dr. Rüdiger Weis ist da allerdings anderer Meinung. Er stört sich schon seit Jahrzehnten am Aufbau und der Funktionsweise von TPM. »Die im TPM 2.0 verwendeten

Resident Evil 8 hatte teilweise massive Performance-Probleme. Die gecrackte Version ohne Denuvo-Kopierschutz lief in einigen Tests besser.

Kryptoverfahren entsprechen nicht dem aktuellen Standard der aktuellen kryptografischen Forschung. Ärgerlich ist, dass trotz möglicher Zusatzkosten von maximal wenigen Cents pro Sicherheitsmodul keine längeren Schlüssellängen als 2.048 Bit verwendet werden«, sagt er uns gegenüber.

Das BSI sieht hier ebenfalls Nachholbedarf, wenn es Microsoft in Zukunft Angreifern nicht allzu leicht machen will. Die staatliche Behörde empfiehlt in einem aktuellen Richtliniendokument, dass verschiedene kryptografische Vorgehensweisen über das Jahr 2022 hinaus eine Schlüssellänge von 3.000 Bit verwenden sollen, »um ein vergleichbares Sicherheitsniveau für alle asymmetrischen Verfahren zu erreichen«.

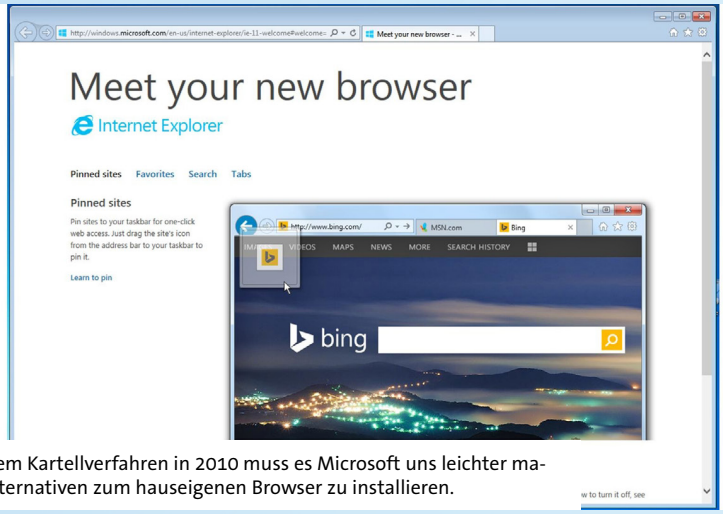
Im letzten Jahr entdeckte ein Wissenschaftsteam aus Deutschland und den USA eine größere Sicherheitslücke, die TPM-Chips von Intel und STMicroelectronics betraf. Beide Firmen haben nach Bekanntwerden den Fehler durch Firmware-Updates ausgebessert. Vor einigen Monaten knackte die Hacker-Gruppierung Dolos Group einen passwortgeschützten Laptop in weniger als 30 Minuten, indem sie eine unsichere Verbindung zwischen TPM und BitLocker ausnutzte. In beiden Fällen handelte es sich um Implementierungsfehler, die nicht direkt die Integrität der TPM-Chips betrafen.

Das BSI teilt auf eine Anfrage mit, dass eine Empfehlung von TPM von den Anforderungen der gewählten Anwendung abhänge. Für die Sicherung einer Festplatte würde sich TPM grundsätzlich anbieten, sagt das BSI. »Allerdings kann auch eine Festplattenverschlüsselung mit einem guten Passwort bereits einen guten Schutz bieten – selbst für einen höheren Schutzbedarf.«

Welche Bedeutung hat TPM im Gaming-Bereich?

TPM kann auch außerhalb der generellen Sicherheit eines Betriebssystems von Nutzen sein. So nutzt etwa der Mediaplayer PowerDVD ein TPM-ähnliches System von Intel, um die Wiedergabe von Ultra-HD-Blu-rays auf

Schon mit Windows 8 erhöhte Microsoft den Druck auf Kunden, TPM zu nutzen.



Seit einem Kartellverfahren in 2010 muss es Microsoft uns leichter machen, Alternativen zum hauseigenen Browser zu installieren.

In Zukunft könnte es immer schwieriger werden, sich dem Microsoft-Kosmos zu entziehen.

Windows abzusichern. Entwicklerstudios und Publisher von Videospielen könnten diese Technologie auch zum Schutz vor Raubkopien und Cheats einsetzen. »Aktuell passiert das so, dass jede Menge Zusatz-Software mit installiert wird, die sich tief im System eingräbt, um es zu überwachen«, sagt Dr. Köpsell. »Das könnte man im Prinzip durch TPM ein Stück weit lösen beziehungsweise besser lösen.«

So gibt es bei dem umstrittenen Kopierschutz Denuvo Hinweise darauf, dass eine fehlerhafte Integrierung der Software Performance-Probleme verursacht. TPM könnte dahingehend eine Alternative sein, auch wenn hier ebenfalls Fehler möglich sind. Zudem wäre das erst in ein paar Jahren ein denkbares Szenario, wenn sich Windows 11 als neues Standardbetriebssystem für Spielende durchgesetzt hat.

Warum setzt Microsoft TPM 2.0 für Windows 11 voraus?

Kryptografieexperte Rüdiger Weis sieht TPM als ein mächtiges Werkzeug an, um Kunden an Microsoft zu binden. »Es entsteht der Eindruck, dass Microsoft mit aller Macht versucht, seine Kunden nach dem Vorbild von Apple in ein geschlossenes System zu zwingen.« Wie bei der Konkurrenz scheinen die Windows-Macher in Zukunft das große Geld mit Abonnementdiensten wie OneDrive, Office 360 oder dem Xbox Game Pass machen zu wollen. TPM kann dahingehend ein Baustein für Microsofts neue PC-Welt sein, die dann alle nicht vom Unternehmen gewollten Programme ausschließt. »Seit fast zwei Jahrzehnten warnen Wissenschaftler vor einem Verlust der Kontrolle über persönliche Computer durch einen TPM-Zwang«, sagt Weis. »Den TPM-Zwang versucht Microsoft mit einer vorhersehbaren Salamitaktik über mehrere Windows-Versionen nun in Windows 11 mit aller Gewalt einzuführen.«

Während man bei Windows 8 TPM noch umgehen konnte, ist dies mit Windows 11 jetzt nicht mehr ohne weiteres möglich. Über Microsofts Vormachtstellung äußert auch das Bundesamt für Sicherheit in der Informationstechnik in seinem Statement vorsichtig kritische Worte: »Das BSI sieht hier in Bezug auf die Transparenz und die Kontrollierbarkeit durch den Plattformeigentümer Verbesserungspotenzial.«

Ist TPM nun schlecht oder nicht?

Die Frage nach gut oder schlecht ist eine schwierige. Kritiker wie Prof. Dr. Weis sehen die reelle Gefahr, dass TPM die Freiheiten des Endkunden massiv einschränken kann, darüber hinaus aber keine wirksame Sicherheit bietet. Außerdem addiert er: »Die Möglichkeit, eigene Programme ohne Genehmigung auf bezahlbarer Hardware zu installieren, hat die ungekannte Geschwindigkeit des technischen Fortschritts erst möglich gemacht.« Das Bundesamt für Sicherheit in der Informationstechnik drückt sich vor einer generellen Empfehlung von TPM und betont, dass es letztlich auf die Implementation ankomme: »Es ist eine Designentscheidung von Herstellern, Sicherheitsfunktionen an das TPM zu binden oder Teilfunktionen in das TPM auszulagern. Wenn hierdurch Nutzer von besser abgesicherten Sicherheitsfunktionen profitieren können, dann ist dies auch aus BSI-Sicht zu begrüßen.«

Dr. Köpsell meint wiederum, dass TPM an sich nicht das Problem sei. »Klar könnte es missbraucht werden, um Nutzer zu entmündigen. Umgekehrt muss man auch ganz klar sagen: Ein wirklich sicheres System ohne einen entsprechend sicheren Hardware-Anker ist schlichtweg nicht möglich. Das heißt, ich brauche so etwas, wenn ich ein wirklich sicheres System will. Die spannende Frage ist, wie setzt man das regulatorisch, organisatorisch um? Wer hat die Kontrolle über die Technologie?« In diesem Fall also Microsoft und Konsorten, die das Zepter in der Hand halten. Wie beim sogenannten Browser-Krieg kann man aber zumindest darauf hoffen, dass sich staatliche Behörden einschalten, sollten die Unternehmen ihre Marktstellung im großen Stil dazu ausnutzen, um die Kundschaft vor vollendete Tatsachen zu stellen. Dass eine Windows-Version von der Öffentlichkeit missbilligt wird, wäre ja auch nicht das erste Mal. Hallo Vista! ★