SCHWARZ
COMPUTER SYSTEME

DEAKTVIERN DES TPM

Deaktvieren des Trusted Plattform Modules

SCHWARZ
Computer Systeme GmbH

Altenhofweg 2a
92318 Neumarkt

Telefon 09181 - 48 55 0
Fax 09181 - 48 55 290

E-Mail info@schwarz.de
www.schwarz.de

AG Nürnberg, HRB 11908
Geschäftsführer:
Manfred Schwarz, Helmut Krauser

Das TPM Module?

I. Was ist das TPM Module?

Die TPM-Technologie stellt hardwarebasierte, sicherheitsbezogene Funktionen bereit. Ein TPM-Chip ist ein sicherer Krypto-Prozessor, der für die Ausführung kryptografischer Vorgänge ausgelegt ist. Der Chip umfasst mehrere physische Sicherheitsmechanismen, die ihn manipulationssicher machen und Schadsoftware ist nicht in der Lage, die Sicherheitsfunktionen des TPMs zu manipulieren. Die wichtigsten Vorteile der TPM-Technologie bestehen in ihren Möglichkeiten. Sie können:

- Kryptografieschlüssel generieren, speichern und deren Einsatz beschränken.
- TPM-Technologie für die Plattformgeräteauthentifizierung nutzen. Sie verwenden dazu den eindeutigen RSA-Schlüssel des TPMs, der in sich selbst geschrieben ist.
- Plattformintegrität gewährleisten, indem Sicherheitsmessungen vorgenommen und gespeichert werden.

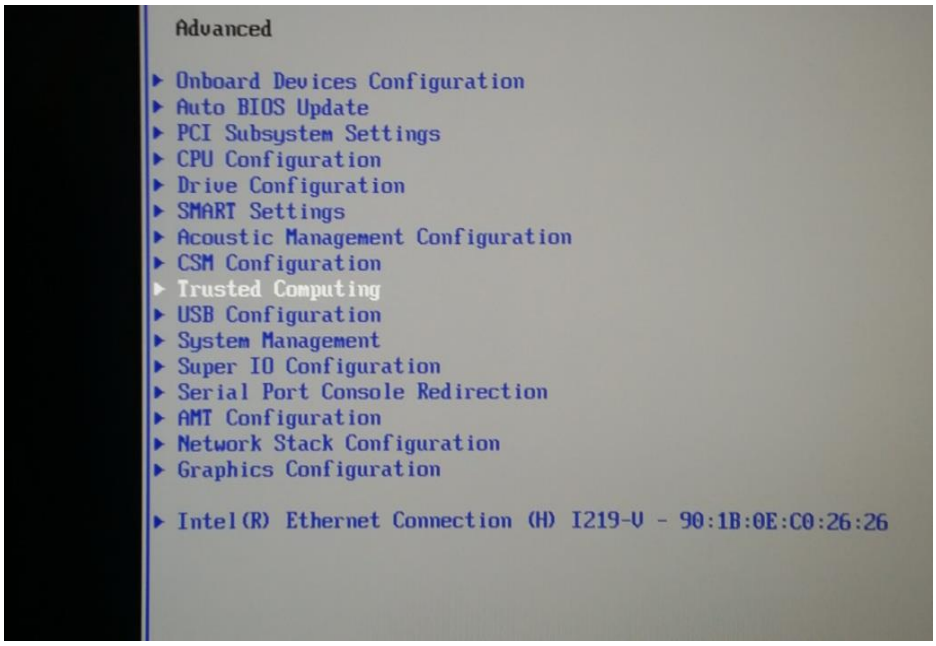
II. Automatische Initialisierung des TPMs mit Windows10

Ab Windows10 wird das Betriebssystem automatisch initialisiert und die Inhaberschaft des TPMs übernommen. Daher empfiehlt es sich in den meisten Fällen, die Konfiguration des TPMs über die TPM-Verwaltungskonsole (**TPM.msc**) zu vermeiden. Es gibt einige Ausnahmen die hauptsächlich mit dem Zurücksetzen oder einer Neuinstallation auf einem PC in Zusammenhang stehen. In bestimmten Unternehmensszenarios (nur Windows 10, Version 1507 und 1511) kann die Gruppenrichtlinie zum Sichern des TPM-Benutzerautorisierungswerts in der Active Directory verwendet werden. Da der TPM-Zustand über Betriebssysteminstallationen hinweg erhalten bleibt, werden diese TPM-Informationen an einem von Computerobjekten getrennten Speicherort in der Active Directory gespeichert. Der TPM Standard wird von Werkseite aus nur von Microsoft Systemen und deren Produkten unterstützt.

Um den PC-SHERIFF nutzen zu können müssen sie auf die Kryptografie des TPM Modules verzichten. Der PC-SHERIFF ist nicht in der Lage den Trustet Plattform Schlüssel welcher vom TPM Module generieret wird zu verwenden. Sie müssen das TPM Module im BIOS deaktivieren.

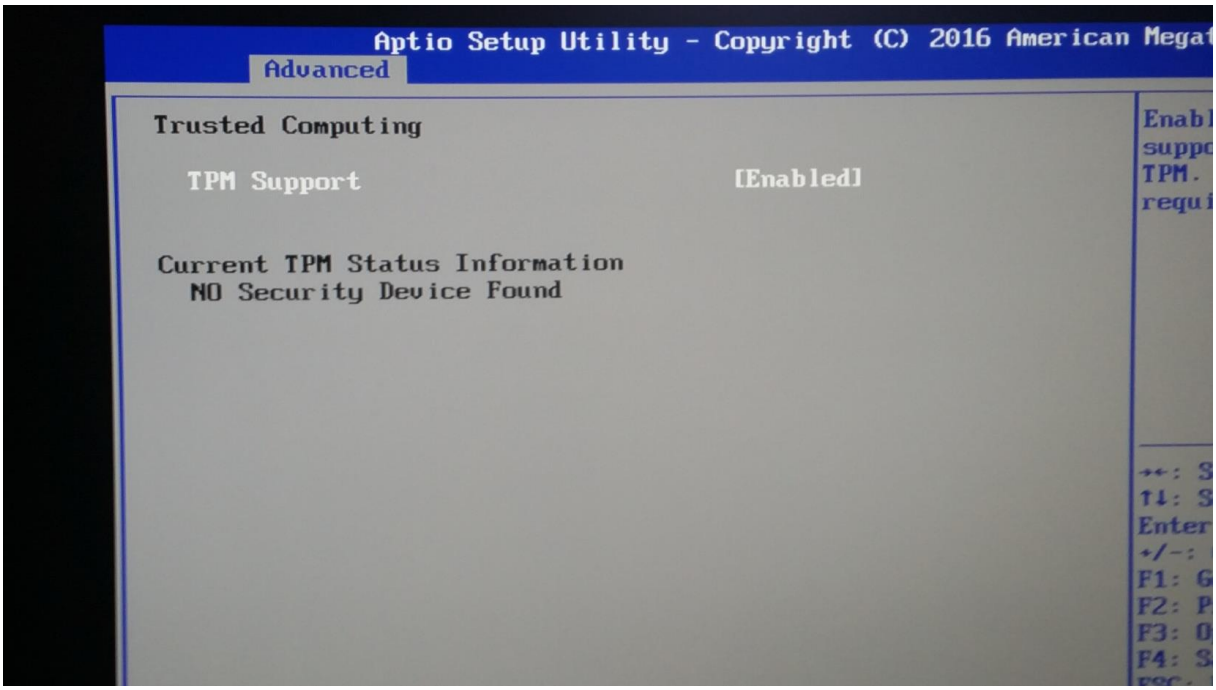
III. Deaktivierung des TPM Modules

Öffnen sie den Reiter Advanced in Ihrem BIO/EVI/UEVI System.

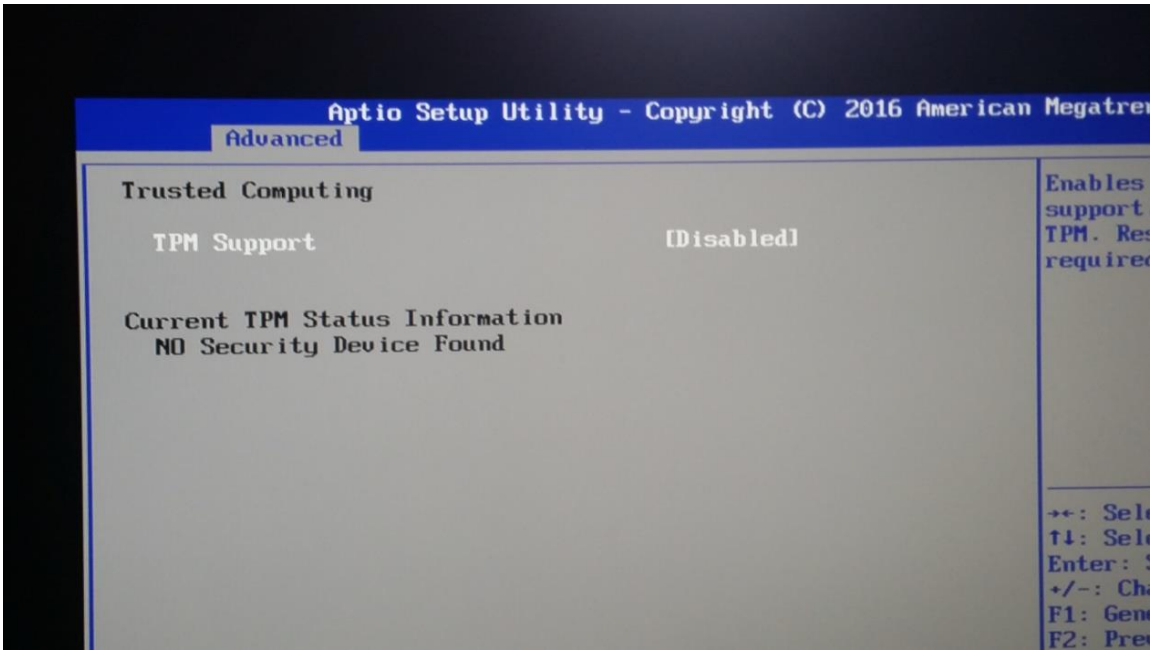


Wählen sie Menü „Trusted Computing" aus. Bestätigen sie mit der Eingabe Taste.

Das Trusted Computing TPM Module wird im Menü TPM Support konfiguriert und ist standardmäßig Enabeld.



Deaktivieren (Disabled) Sie den TPM Support indem sie die Eingabe Taste betätigen und mit den Pfeiltasten die Einstellungen verändern. Wenn Disabeld angezeigt wird bestätigen Sie dies mit der Eingabe Taste. Das TPM module ist nun deakiviert.



Sie müssen als letzten Schritt die Änderungen im BIOS speichern. Speichern Sie die Änderungen mit der F10 Taste. Bestätigen Sie die nachfolgende Abfrage mit „J". Sollte die Deutsche Tastatur nicht erkannt werden, gilt die US Tastaturbelegung. In diesem Fall bestätigen Sie die Abfrage mit „Z". Verlassen Sie anschließen das BIOS Menü und Starten Sie den PC neu.

Quellen:

www.technet.microsoft.com/tpmandtrustedcomputing

www.schwarz.de/support