Verwaltungsgericht Cottbus
Vom-Stein-Straße 27
03050 Cottbus
Telefax: 0355 4991-6499
Doppelte Ausführung
AZ: VG 8 K 556/21

Von:
Marcel Langner
[redacted]

Sehr geehrte Vorsitzende Richterin, sehr geehrte Kammer,
mich erreichte am 03.09.2021 Ihr Schreiben vom 31.08.2021 mit Anhang der Hochschule und Bitte um Stellungnahme.
Ich habe das Gefühl, dass mit jedem Schreiben immer ein Stückchen mehr der aktuellen Situation an dieser Hochschule an das Tageslicht kommt. Ich möchte gern vermuten, dass auch Sie, wertes Gericht, nicht vollständig von der Argumentation der Hochschule überzeugt sind und mir deshalb die Chance zur Stellungnahme einräumen.

Ich habe die fachlichen Argumente der Hochschule in Anlage 1 widerlegt, ebenso eventuelle Missverständnisse im Verständnis meiner Argumente. Viele Aussagen der Hochschule erschließen sich mir nicht. Ich finde diese Fachdiskussion jedoch aktuell nicht mehr zielführend, da mir unabhängig von der Stichhaltigkeit (jeder Seite) das Recht auf Akteneinsicht nicht mehr tangiert zu werden scheint.

Ganz entschieden möchte ich jedoch der möglicherweise irreführende Aussage:
„Reputationsfilter sind keine händisch gepflegten Sperrlisten oder „Blacklisten" und somit auch nicht vergleichbar in Anwendung und Wirkung.“
in dieser Allgemeinheit entgegentreten und kann nur Vermutungen anstellen, wie diese gemeint sein könnte.
Innerhalb des Systems, in dem eine IP Filterliste eingesetzt wird, hat sie eine Funktion: Zugriffe auf IP Adressen zu verweigern. Es ist komplett unerheblich für diese Anwendung (Zugriff auf IP Adressen verweigern), ob diese Liste dynamisch (z.B. über ein Reputationssystem oder Künstliche Intelligenz) erstellt wurde oder ob ein Mensch diese „händisch“ angelegt hat. Im System in dem die Sperrung durchgeführt wird ist es eine schlichte Liste von IP Adressen, die hier im Kontext der Sperrung synonym auch als Sperrliste oder „Blackliste“ bekannt (20.07.2021) ist.
Unklar bleibt bei mir auch, was sich hier nicht vergleichen ließe. Die Hochschule tut dies sogar selbst, in dem sie in ihrer folgenden Argumentation auf die Vorzüge dynamisch erstellter Sperrlisten gegenüber „händisch“ erstellten abzielt.
Hier kann ich nur vermuten, dass die Hochschule damit meint, dass bei dynamischen Listen nur jemand einen Haken in einer Benutzeroberfläche setzen muss, anstatt in eine Liste IP Adressen einzutragen. Warum Anwendung/Wirkung hier aber nicht vergleichbar sein sollen erschließt sich mir nicht. Damit liegen auf den Systemen der Hochschule IP Filterlisten vor und sind Akten im Sinne des AIG. Dass die Hochschule an diese unter Umständen nicht leicht herankommt ist eine andere Frage, erklärt jedoch nicht warum sie dann meine Anfrage (30.08.2021) mit „Es liegen keine entsprechenden Fälle vor.“ beantwortet.

Die Hochschule gibt an, die genauen IP Adressen überhaupt nicht zu kennen. Ich möchte vorab auf Anlage 2 verweisen. Hier befinden sich öffentlich einsehbare Beispiele für einen Anbieter von Reputationsfiltern mit Erläuterungen, welche Möglichkeiten diese Filter überhaupt anbieten. Da die Hochschule vorrangig Produkte vom US Unternehmen Cisco einsetzt, vermute ich, dass tatsächlich auch der genannte Anbieter genutzt wird. Die eingesetzten Cisco Produkte werden von Talos auch als

Datensammler genutzt, liefern also auch selbst Telemetriedaten, die dann widerum für die dynamischen IP Filterlisten genutzt werden. Dazu schreibt Talos in seinem Whitepaper:
„Cisco Talos has more visibility than any other security vendor in the world, with the sheer size and breadth of the Cisco Security portfolio and the incoming telemetry from Cisco's customers and products."
Eventuell als fehlerhaft erkannte Sperren lassen sich auf der Webseite des Anbieters mithilfe eines Kundenlogins melden. Diese werden dann „händisch" aus den Listen ausgetragen bzw. überprüft oder auch „händisch" hinzugefügt. In diesem Sinne schätze ich diese Filterliste als eine Art Hybriden ein, welche dynamische und „händische" Komponenten aufweist.

Erst jetzt erläutert die Hochschule, dass sie IP Filterlisten ausschließlich vollautomatisch und damit ungeprüft in ihre Systeme einspielt und deren Inhalt daher nicht konkret kennt und diese Listen auch dynamisch zusammengestellt werden. Ich bin schon der Ansicht, dass es möglich ist, eine Filterliste zu einem bestimmten Zeitpunkt aus den Systemen zu extrahieren oder eine Kopie der Originalquelle zur Verfügung zu stellen. Da diese sich jedoch ständig ändern, ist ein Snapshot aber nur von wenig Wert für mich. Mir geht es ja darum Akteneinsicht in jene Aufzeichnungen zu nehmen, aus denen die andauernden Grundrechtseinschränkungen hervorgehen und wie stark diese sind. Ich schlage daher vor (als für mich akzeptable Teilauskunft) über folgende Sachverhalte Auskunft zu erteilen, wobei ich diese Auskunft ohne meinen Vorschlag, im Rahmen der Auslegung meines Antragsgegenstandes, von der Hochschule erwartet hätte (§6 (1) AIG, Unterstützung):

- Welche konkreten Filterlisten (Name, Bezeichnung) welcher Anbieter werden eingesetzt bzw. wurden bisher eingesetzt? (Wenn verfügbar ein Link zur Quelle)
- Welche Bedrohungslevel sind aktuell aktiviert?
- Welche Kategorien sind aktuell aktiviert?
- Welche Inhaltsfilter sind aktuell aktiviert?
- Welche weiteren Art(en) von Filter werden eingesetzt? (DNS Sperren usw...)

Alle diese Informationen müssen in Systemen eingestellt werden und werden in diesen gespeichert. Sie stellen damit Akten im Sinne des AIG dar. Da meine ursprüngliche Anfrage (30.08.2020) auch die Gründe für Sperren erfragte, würde ich die Bedrohungslevel/Kategorien hier als Teilauskunft bezeichnen und frage mich auch hier, warum diese bisher nicht beauskunftet wurden. In der praktischen Umsetzung könnte die Auskunft durch z.B. Screenshots der Benutzeroberflächen erfolgen, sofern wirklich keine explizite Dokumentation vorliegt.
Diese Auflistung kann nur beispielhaft sein, da mir die Eigenschaften/Strukturierung der anderen eingesetzten Sperrfilteranbieter nicht bekannt sind. Ich hoffe aber nun erneut dargelegt zu haben, wo sich die Motivation meiner Anfrage befindet. Dies müsste auch der Hochschule, so unangenehm ihr diese Informationen auch sein mögen, eigentlich aufzeigen, welche weiteren Informationen noch davon betroffen sein könnten. Ihre ursprünglich vertretenen fachlichen Ansichten, es handele sich um eine Sicherheitsproblematik, hat sie bisher nicht wiederholt.
Sofern sich Verweise auf öffentliche Quellen ermöglichen, wo ich die (jeweils aktuellen) Daten/Listen selbst herunterladen kann und diese auch jene sind, die hier von meiner Anfrage konkret erfasst sind erachte ich §6 (4) AIG als einschlägig an (Selbstbeschaffung). Diese Verweise sollten jedoch auf die konkret relevante Quelle zeigen.

Ich konnte in der Erwiderung der Hochschule auf meine folgenden Argumente keine Antwort finden:

- Meiner Erfahrung nach sind mehr Ports gesperrt, als angegeben. Bisher liegt mir die Akte, nach der die Hochschule mit ISO27001 A7.5/A7.5.3 abwehrend argumentiert (22.12.2020) nicht vor. Das dort nur enthalten sein soll: TCP Port 23, halte ich für ausgeschlossen. Ich bin sicher Zeugen auftreiben zu können, die bestätigen, dass auch jetzt immer noch weit mehr Ports gesperrt sind, als die Hochschule hier angegeben hat. Hier mit der Bitte an das Gericht, deren Anonymität gegenüber der Hochschule zu wahren.

- Sind auch Dienste (z.B. URLs, Domains) von Sperrungen betroffen oder wirklich nur IPs?

Dann gibt die Hochschule überspezifiziert bestimmte Netzwerke an (20.07.2021). Gibt es weitere Netzwerke die einen Zugriff von innerhalb nach außen zulassen? Ich kann die Bezeichnung/Struktur der unterschiedlichen Netze ja nicht kennen, da auch zu meiner Zeit an der Hochschule alle Anfragen bezüglich solcher Themen als „sicherheitskritisch“ eingestuft und nicht beantwortet wurden.

Bei der Zertifizierung nach ISO27001 gibt es zwei Varianten. Einmal die ISO27001 und zum anderen die ISO27001 auf Basis des IT Grundschutzes. Dazu führt die Webseite https://www.myrasecurity.com erläuternd aus:
„Unternehmen können sich ihre umgesetzten Sicherheitsmaßnahmen mit einer offiziellen Zertifizierung nach ISO 27001 beziehungsweise ISO 27001 auf Basis von IT-Grundschutz bescheinigen lassen. So machen sie nach außen sichtbar, dass sie definierte Sicherheitsstandards erfüllen. Das schafft Vertrauen bei Kunden und Partnern.
ISO 27001 auf Basis von IT-Grundschutz bietet hier einige Vorteile. Einer besteht darin, dass es konkrete Vorgaben gibt, welche Sicherheitsmaßnahmen wie umzusetzen sind. Eine erfolgreiche Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz sagt also nicht nur aus, dass ein ISMS vorhanden ist, sondern auch, wie es im Detail ausgestaltet wurde. Auftraggeber, Partner und Kunden eines nach ISO 27001 auf Basis von IT-Grundschutz zertifizierten Dienstleisters können die vorhandenen Sicherheitsmaßnahmen somit von außen einschätzen. Eine reine ISO-27001-Zertifizierung erlaubt diese Einschätzung nicht, da die allgemeinen Vorgaben nicht einheitlich umgesetzt werden.“

Soweit ich erkennen kann besitzt die Hochschule nicht die Zertifizierung auf Basis des IT Grundschutzes. Sie kann daher recht frei und willkürlich entscheiden, welche konkreten Umsetzungen sie zur Zielerreichung vornimmt, da die ISO27001 ohne IT Grundschutz Zertifizierung genau dies eben nicht überprüft. Das zeigt auch, dass die Hochschule recht flott eine Neubewertung der Gefährdungslage vornehmen kann, ohne das es (entgegen ihrer eigene Aussage (22.12.2020)) Probleme mit der Zertifizierung gibt (28.07.2021).
Es ist mir daher ohne die Einsicht in die Zertifizierungsunterlagen nicht möglich von außen zu ermitteln, welche Rollenzuordnungen existieren und wer diese innehat und welche Rollen es überhaupt gibt. Nur mit diesen ist jedoch nachweisbar, dass sehr wohl Personen ermittelbar sind, die, wenn auch nur ableitbar, dokumentiert die Berechtigung besitzen die Quellen der IP Filterlisten und Einstellungen festzulegen und welche Verantwortlichkeiten vorliegen. Es ist nicht glaubhaft, dass nirgendwo veraktet ist, wer Zugriff auf die Systeme hat und wer nicht und wer formal die Verantwortung für IP Sperrlisten trägt. In dem Sinne ergeben sich die Zugangsberechtigungen natürlich auch aus den direkt in den Systemen zugeordneten Berechtigungsstufen. Das sind ja auch amtlichen Zwecken dienende Information mit Vorgangsbezug nach AIG. Sollten sich meine Fragen dahingehend nur aufgrund der vergebenen Berechtigungen ableitend beantworten lassen, so würde mir eine einfache Auskunft reichen. Wer dann real wirklich die Änderungen durchführt, kann ich dadurch dann zwar nicht ermitteln, aber wenn die Hochschule angibt keinen verakteten Prozess dazu zu besitzen, dann ist das zumindest eine Teilauskunft (die ich auch bereits erwartet hätte).
Die bisherigen Auskünfte waren der Hochschule nur dadurch abzuringen, dass ich irgendwie nachweisen konnte, dass die Unterlagen existieren (z.B. das Verfahrensverzeichnis). Erst im Verfahren kam dann noch heraus, dass doch IP Filterlisten eingesetzt werden. Vielleicht kann das werte Gericht nachvollziehen, dass mein Vertrauensvorschuss gegenüber der Hochschule im Kredit steht und ich Behauptungen, es gäbe eine bestimmte Unterlage nicht, kritisch gegenüber stehe.

[redacted]

Anlage 1: Widerlegte Behauptungen der Hochschule, Aufklärung Missverständnisse

Ich gehe im Moment davon aus, dass wir einer ausreichend gleichen Definition des Begriffes Reputationsfilter folgen, da ich die Erläuterung der Hochschule nicht als zu stark von meiner als abweichend empfinde (2-10).

5
Die ermittelten IP Adressen sind nicht ausschließlich Schadsoftwarequellen. Es finden auch andere Kategorisierungen (auch ohne Schadpotenzial) statt (siehe Anlage 2). Die genaue Art und Weise der Einstufung wird vermutlich ein Geschäftsgeheimnis sein und kann daher nicht transparent nachvollzogen werden.

6
Ja das kann durchaus möglich sein. Ich halte die Wahrscheinlichkeit genau dieses einen speziellen Falles, wie unten (13+14) erläutert, jedoch für wenig häufig. Mir sind keine Belege/Studien dazu bekannt.

8
Ich verstehe diesen Punkt so, dass er sich auf Systeme bezieht, die Daten von außen in die Hochschule senden wollen. Hier z.B. Spam Emails bei der Hochschule einliefern wollen. Diese Verbindungsrichtung ist und war nicht Teil meiner Anfrage.

11
Eine Dokumentation hatte ich auch nicht verlangt. Ich wollte nur die Liste selbst. Dass diese jedoch vorliegt und somit eine Akte im Sinne des AIG ist, habe ich zuvor ausgeführt.
Nicht nachvollziehen kann ich die Aussage, warum eine automatische Aktualisierung eine Manipulation verhindern soll. Sowohl der Anbieter kann die IP Liste manipulieren, als auch Angestellte oder Angreifer, sofern die Verbindung zum Anbieter nicht nach Stand der Technik verschlüsselt und authentifiziert ist. Warum durch einen Automatismus die Leitung eines Nutzers (wer ist damit überhaupt gemeint?) nicht belastet wird, habe ich garnicht verstanden. Die Liste (bzw. ein Diff) muss doch durch die Leitung, um im System eingespielt werden zu können.

13+14
Ich will meine Argumentation hier so verstanden wissen, dass ein wie hier von der Hochschule beschriebenes Szenario nicht auch möglich ist. Ich halte es aber, wie auch ein Angriff von Aliens, für eben unwahrscheinlich. Die Grundlinie der Argumentation bezüglich „Sicherheit“ entspricht damit auch den sich wiederholenden Aussagen der Hochschule. Hier bei jeglicher denkbaren Gefahr auf Verdacht zu sperren. Dieser Argumentation konnte auch die BNetzA fachlich nicht folgen, als die Hochschule angab, aus Sicherheitsgründen alle anderen WLAN Signale auf ihrem Gelände aktiv stören zu müssen.
Bis auf die Schlussfolgerungen, scheint es mir jedoch, als ob mir die Hochschule fachlich zustimmt, da ich prinzipiell nichts anderes lese, als ich auch geschrieben habe. Tatsächlich widerspricht sie sich meiner Lesart nach in 16 auch selbst. Erst sind C&C Server sehr lange im Netz (unbelegtes Gegenargument zu meiner auch unbelegten Vermutung) erreichbar, um danach schnell durch andere ersetzt zu werden (Begründung für Reputationslisten und meiner Argumentation folgend). So wie es eben passt. Das ist letztlich das, worauf ich hinauswollte. Es geht um Wahrscheinlichkeiten und die Schlussfolgerungen daraus. Hier wird es bei unüberbrückbaren Ansichten über zulässige und nicht zulässige Grundrechtseinschränkungen bleiben, die mir jedoch in der Klärung nicht zum Zugang nach AIG hilfreich erscheinen.

15+16
Die Hochschule begründetet ihre Sperrung des TCP Ports 23 ursprünglich damit, dass man sich darüber in entfernte Systeme einloggen kann (Dienst Telnet-Server/Client) und dabei das Passwort (und alle anderen Daten) unverschlüsselt übertragen wird (20.07.2021). Deshalb erwähnt sie auch den Dienst SSH als

Alternative zum Dienst Telnet-Server/Client, der genau das auch macht, aber verschlüsselt. Auf dieser Basis ist auch meine Argumentation zu verstehen. Dass eben der Dienst Telnet-Server/Client (der tatsächlich auch auf einem beliebigen anderen Port laufen kann) heutzutage nicht mehr im Internet eingesetzt wird. Ausgangspunkt für mich ist immer der Normalfall: Stand der Technik. Diese Argumentation wiederholt sie nicht, sondern hat wieder was neues im Gepäck und erweitert nun dahingehend, dass der Port 23 unabhängig von dem Dienst der darüber läuft gefährlich sein könnte und oftmals durch Dritte zweckentfremdet wird. Dort kann ich dahingehend zustimmen, dass Port und Dienst eben nicht zwangsläufig gekoppelt sind. Port 23 wird auch noch genutzt und ja das kann auch Schadsoftware sein, die aber auch jeden anderen Port nutzen kann, den sie möchte. In dem Sinne unterscheidet sich Port 23 nicht von vielen anderen Ports (Vergleich mein Telefonbeispiel 20.05.2021).

Damit kann ich auch der Schlussfolgerung der Hochschule bezüglich ihrer Grafik komplett nicht folgen.
Sie gedenkt diese als Nachweis dafür zu erbringen, dass auf Basis des Argumentes der Zweckentfremdung des Ports 23 für einen anderen Dienst bei nachlässigem Umgang (hier also ohne Blocks) das komplette Netzwerk (der Hochschule) durch einen Angriff kompromittiert werden könnte. Kurz: Wenn wir nicht blocken würden, besteht die Gefahr, dass das komplette Netzwerk kompromittiert werden könnte.
Auch hier bleibt in der Konsequenz dieses unbelegten Konjunktivs totaler Sicherheit damit nur die Sperrung aller Ports.
Ich sehe nicht warum sich Port 23 hier von allen anderen Ports unterscheiden sollte, die ja auch zweckentfremdet werden können. Ein wenig erklärbar wäre es mir, wenn die Hochschule hier den Fall beschreibt, dass die Verbindung von außen zur Hochschule gerichtet ist. Dann hätte die Hochschule selbst Systeme im Internet, die Port 23 geöffnet haben und dieser auch noch zweckentfremdet wird oder den Dienst Telnet-Server/Client am laufen hat. Dafür wäre auf jeden Fall Schutz angebracht. Diese Verbindungsrichtung ist und war aber nie Ziel meiner Anfragen. Ich will wissen, welche Sperren aus dem Netz der Hochschule in das Internet gerichtet sind.

Damit kann ich auch zur Grafik nur sagen, dass mir nicht ermittelbar ist, ob wir hier die geblockten Verbindungsversuche von innerhalb der Hochschule nach außen, oder von außerhalb zur Hochschule sehen. Und von welchen Netzwerkübergängen diese Daten überhaupt stammen.
Unklar bleibt auch, ob es sich hier um ein typisches und damit überhaupt argumentativ unterstützendes Muster handelt. Ebenso wie dieses aufgezeichnet wurde und welche Datenquellen wie zusammengeführt wurden.

Rechnersysteme im Internet werden kontinuierlich gescannt. Auch auf Port 23. Von Angreifern, Sicherheitsfirmen, Sicherheitsforschern, Hackern usw. Verbindungsversuche von außen zur Hochschule sind daher nicht ungewöhnlich. Meiner Erfahrung nach sind dies dann sogar noch recht wenig. Dabei wird jedoch nicht nur Port 23 gescannt, sondern praktisch immer sehr viele/alle Ports. Die Scannenden wissen nämlich auch sehr genau, dass Port und Dienst nicht fest miteinander gekoppelt sind.

Für den Fall, dass die Grafik nun doch die geblockten Verbindungsversuche von innerhalb des Netzwerkes der Hochschule nach außerhalb aufzeigt finde ich das Muster der Verbindungsversuche ungewöhnlich. Das Muster ist nämlich über den gesamten Tagesverlauf relativ gleichmäßig, was bei kontinuierlichen Portscans von außerhalb ein übliches Muster ist. Da wir Menschen ja üblicherweise schlafen gehen und dann die Rechner (meistens) auch ausschalten, müsste irgendeine Form dieses Tages-/Nachtrhythmus eigentlich erkennbar sein, sofern die Blocks von innen nach außen gerichtete Verbindungsversuche zeigen. Das ist nur wenig ausgeprägt. Es gibt also dann im Bereich der Hochschule Rechnersysteme die ständig eingeschaltet sind (vermutlich Serversysteme), die dauerhaft versuchen auf Port 23 Verbindung nach außerhalb aufzunehmen. Wo genau bleibt jedoch unklar, da die Netzstruktur nicht offengelegt ist und somit auch hier die Aussagekraft schlecht einzuschätzen ist.

Und letztlich zeigt die Grafik dann irgendwelche geblockten Verbindungsversuche auf Port 23. Das zeigt doch aber nicht, dass diese Verbindungsversuche der Dienst Telnet-Server/Client sind oder eine Gefahr darstellen oder Schadsoftware sind.
Es könnte sich auch schlicht um fehlkonfigurierte Systeme der Hochschule handeln. Denkbar sind auch Systeme von Forschenden, die selbst das Internet scannen und nun daran gehindert werden. In den Daten solcher Forschenden wird der Port 23 nun in einer Statistik als nicht zugreifbar auftauchen und könnte damit zu fehlerhaften Schlussfolgerungen führen, da ja auch diesen nie gesagt wurde, welche Ports gesperrt sind.
Die Datenaufnahme und -aufbereitung, die hier für die Grafik durchgeführt wurde, könnte auch selbst fehlerhaft erfolgt sein. Ich möchte daher dieser Grafik und der Schlussfolgerung der Hochschule wenig bis keine Beweiskraft zurechnen, solange die von mir aufgeworfenen Fragen nicht geklärt sind.
Ich denke aber auch, dass die Klärung hier nicht zielführend zur Akteneinsicht nach AIG ist.

Anlage 2: Optionen von Filterlistenanbietern; hier Talos Intelligence (Cisco Tochter)
Entnommen der Webseite https://talosintelligence.com

Die Beispiele zeigen, welche Inhaltsfilter zur Auswahl stehen und auf welcher Basis man diese aktivieren kann, also z.B. welches Bedrohungs Level oder Kategorien man gern blocken möchte.

Beispiele (aus 106) für Inhaltskategorien für Filter (sinnerhaltend in Faxkompatibles Format übertragen): (https://talosintelligence.com/categories#contentcats)

Category	Abbreviation	Code	Description	Example URLs
Adult	adlt	1006	Directed at adults, but not necessarily pornographic. May include adult clubs (strip clubs, swingers clubs, escort services, strippers), general information about sex, non-pornographic in nature, genital piercing, adult products or greeting cards, information about sex not in the context of health or disease.	http://www.adultentertainmentexpo.com http://www.sincerelynot.com
Advertisements	adv	1027	Banner and pop-up advertisements that often accompany a web page, other advertising websites that provide advertisement content. Advertising services and sales are classified as Business and Industry.	http://www.adforce.com http://www.doubleclick.com
Child Abuse Content	cprn	1064	Worldwide illegal child sexual abuse content.	
Personal VPN	pvpn	1102	Virtual private network (VPN) sites or tools that are typically for personal use,and, may or may not be approved for corporate usage.	http://www.openvpn.net http://www.torvpn.com

Beispiele (aus 20) von Bedrohungs-Kategorien (sinnerhaltend in Faxkompatibles Format übertragen): (https://talosintelligence.com/categories#threatcats)

Category	Description
Malware Sites	Websites that are known to contain, serve, or support malware in its delivery, propagation, or in carrying out its malicious intent.
Spam	Known to serve, deliver or aide in the propagation of Spam.
Open HTTP Proxy	Hosts that are known to run Open Web Proxies and offer anonymous web browsing services.
Malicious Sites	Sites exhibiting malicious behavior that do not necessarily fit into another, more granular, threat category.

Bedrohungs Level für Webseiten Reputation (sinnerhaltend in Faxkompatibles Format übertragen):
(https://talosintelligence.com/reputation_center/support#faq3)

Legacy Verdict	New Threat Level	Description
Good	Trusted	Displaying behavior that indicates exceptional safety
Neutral	Favorable	Displaying behavior that indicates a level of safety
	Neutral	Displaying neither positive or negative behavior. However, has been evaluated.
	Questionable	Displaying behavior that may indicate risk, or could be undesirable
Poor	Untrusted	Displaying behavior that is exceptionally bad, malicious, or undesirable
Unknown	Unknown	Not previously evaluated, or lacking features to assert a threat level verdict