CERT News

Alles im grünen Bereich?!

Bei einer Ampel weiß jeder, was Grün und Rot bedeuten. Auch für die Sicherheit im Internet gibt es entsprechende „Lichtsignale", die auf den ersten Blick einleuchtend erscheinen – doch wie passend ist die Symbolik wirklich?

Die Quintessenz eines IT-Sicherheitslagebilds kurz und prägnant zu erfassen ist nicht leicht. Daher werden gerne Analogien bemüht: Bilder, mit denen Menschen aus anderen Bereichen vertraut sind – insbesondere Ampeln und Barometer. Bei näherer Betrachtung sind diese allerdings nur begrenzt in der Lage, den angestrebten Zweck zu erfüllen.

Es gibt heute eine ganze Menge solcher Indikatoren, die mit grafischen Hilfsmitteln eine zusammenfassende Bewertung des IT-Sicherheitsstatus liefern wollen – zwei sollen hier exemplarisch einander gegenüber gestellt werden: Einer der ältesten ist sicherlich der „Internet-Threat-Level" des Internet Storm Center (http://isc.sans.org/infocon.html). Und hierzulande hat seit einiger Zeit der Verein „Deutschland sicher im Netz" (DsiN, www.sicher-im-netz.de) einen Online-Sicherheitsstatus definiert, der dasselbe Ziel verfolgt: Menschen für sicherheitskritische Veränderungen zu sensibilisieren und gegebenenfalls deutlich zu warnen.

Vergleicht man die Definitionen der beiden Indikatoren, so gibt es jeweils vier Stufen (in Tabelle 1 mit A bis D bezeichnet), die in beiden Fällen die gleiche Farbe haben, allerdings nicht durchgängig das Gleiche bedeuten. Die Farben orientieren sich an den Ampelfarben Grün, Gelb und Rot – als Viertes kommt noch Orange hinzu (einigen Autofahrern aus Beifahrerkommentaren oder als Entschuldigung ebenfalls bekannt).

Gleich und ungleich

Bereits anhand der Definitionen wird schnell klar, dass beide Indikatoren ein unterschiedliches Zielpublikum anpeilen. Besonders deutlich wird dies bei der Stufe Rot: Im Fokus des deutschen Sicherheitsbarometers stehen Endanwender – das ISC betrachtet hingegen vorrangig die Nutzbarkeit der Infrastruktur „Internet".

Wirklich oft sagt ein Bild mehr als tausend Worte. Dies ist genau der Grund, warum so gerne die Ampel-Symbolik genutzt wird: Sie ist quasi allen Menschen in der westlichen Hemisphäre bekannt und vertraut – im Laufe unseres Lebens haben wir gelernt, das wir bei Grün gehen können und bei Rot anhalten müssen. Selbst wer Ampeln als Fußgänger tendenziell ignoriert, legt doch bei Rot (hoffentlich) besondere Vorsicht an den Tag...

Nun ist es leider bei den hier vorgestellten (aber auch vielen anderen) Indikatoren aber nicht so, dass die Farbe Grün uns eine „sichere Passage" verspricht. Schon die Definitionen besagen: Grün heißt nicht etwa „kein Risiko", sondern bedeutet nur „normale" Gefahr. Man mag einwerfen, dass man auch bei einer grünen Verkehrsampel nicht ohne nach rechts und links zu schauen über die Straße gehen sollte. Dennoch bleibt die Frage, was schwerer wiegt: Das Wissen um ein gewisses Restrisiko oder die über viele Jahre erlernte Entspannung (wenn nicht Sorglosigkeit), die „Grün" für uns bedeutet.

Tabelle 1: Gefährdungsstufen im Vergleich

Stufe	Farbe	Deutschland sicher im Netz	Internet Storm Center
A	Grün	Die Stufe Grün wird als „normales Risiko" bezeichnet.	Alles ist normal, keine signifikanten neuen Bedrohungen sind bekannt.
B	Gelb	Die Stufe Gelb wird als „erhöhtes Risiko" bezeichnet und hat die Aufgabe, die Nutzer vor akuten Bedrohungen zu warnen, deren Verbreitung oder Schadensausmaß allerdings begrenzt sind. Gelb kann aber auch den dringenden Bedarf zum Schließen von Sicherheitslücken mit kürzlich verfügbar gewordenen Sicherheits-Updates unterstreichen.	Es wird aktuell eine signifikante neue Bedrohung beobachtet, deren Auswirkungen entweder noch unbekannt sind oder nur wenig Einfluss auf die Internet-Infrastruktur haben wird. Trotzdem können die lokalen Auswirkungen signifikant sein und Benutzern wird geraten, sofort bestimmte Schritte einzuleiten, um Schäden zu minimieren.
C	Orange	Die Stufe Orange wird als „hohes Risiko" bezeichnet und hat die Aufgabe, die Nutzer vor akuten Bedrohungen zu warnen, deren Verbreitung oder Schadensausmaß signifikant sind.	Eine größere Störung der Konnektivität steht bevor oder ist bereits eingetreten.
D	Rot	Die Stufe Rot wird als „Internet-Alarm" bezeichnet und soll die Nutzer vor aktuellen Bedrohungen warnen, die Verfügbarkeit oder Integrität von PCs und Netzwerken in großem Ausmaß gefährden.	Verlust der Konnektivität in großen Teilen des Internets.

Streng genommen dürfte eine Ampel zur IT-Sicherheitslage heute nie auf Grün stehen – und was nützt eine solche Ampel dann?! Eine wichtige Eigenschaft von (Verkehrs-)Ampeln ist ja, dass diese etwas regeln und auch nach einer gewissen Zeit umschalten, also beispielsweise dem Querverkehr grünes Licht geben. Nun möchte aber niemand den Angreifern „grünes Licht" geben...

Und auch beim Rot stimmt das Bild nicht: Im Verkehr haben wir gelernt, bei Rot stehen zu bleiben – Zuwiderhandeln ist zu gefährlich, jedenfalls zu den Hauptverkehrszeiten. Doch im Netz bleibt man sehr lange nicht (freiwillig) stehen! Solange es irgendwie geht, bleibt man mit dem Internet verbunden und auch (oder gerade) die elementaren, für das Geschäft wichtigen Server werden weiter betrieben, ob es nun neue Angriffe gibt oder nicht...

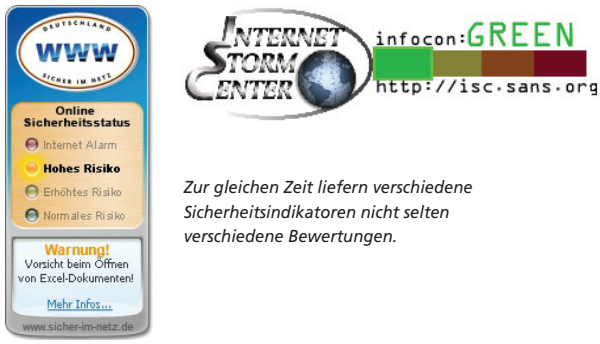
Griechen und Trojaner

Wir Informatiker sind bisweilen auf der Suche nach anschaulichen Bildern wenig wählerisch. Wir haben oft nichts dagegen, unterschiedliche Begriffe für gleiche Dinge zu verwenden oder durch einen neuen Begriff Aufmerksamkeit für ein altes Konzept zu schüren. Ein Beispiel: Der Bot (im Bot-Netz) ist ja eigentlich gar kein unabhängig agierender Roboter, sondern eher die Tentakel-Spitze eines vielarmigen Oktopus – und letztlich handelt es sich schlicht um einen Trojaner, der früher einmal Trojanisches Pferd hieß (und dessen historisches Vorbild Griechen verbarg).

An sich spricht „Deutschland sicher im Netz" ja auch gar nicht von einer Ampel, sondern vom Sicherheits-Barometer – und das „Internet Storm Center" zielt schon im Namen auf die Großwetterlage im Netz ab. Die Metapher des Barometers ist vielen ähnlich vertraut wie eine Ampel – bei einem „Hoch" rechnen wir mit schönem Wetter, während bei einem „Tief" zuhause bleiben oder zumindest ein Regenschirm angesagt sind. Tatsächlich ist es schwierig, die Genauigkeit eines Barometers, das exakt in Millibar misst, bezüglich der Sicherheit im Internet zu errreichen – daher haben sich beide Indikatoren auf vier Stufen und die Farben der Ampel zurückgezogen, die Bilder also gemischt.

Auch wenn die Ampel als Bild für den Sicherheitsstatus nicht wirklich geeignet ist, bleibt sie doch universell und unmittelbar verständlich: Man muss die Ordnung der Farben nicht lange erklären, jeder wird (zumindest) verstehen, dass Rot schlechter ist als Grün. Dafür sorgt auch die psychologische Wirkung der Farben: Rot gilt als aggressiv und gefährlich, Grün als beruhigend.

Für Experten, die über all die genannten Eigenheiten informiert sind, funktionieren die Indikatoren ohnehin. Experten nutzen sie als groben Anhalt und erwarten



Zur gleichen Zeit liefern verschiedene Sicherheitsindikatoren nicht selten verschiedene Bewertungen.

keine Aussage über konkrete Bedrohungen: Wenn es Grün ist, kann „natürlich" trotzdem etwas passieren, und auch wenn es Rot ist, muss eine einzelne Organisation nicht von dem betroffen sein, was an anderer Stelle geschieht. Experten berücksichtigen bei der Bewertung eines Indikators ihre Erfahrungen; dabei geht ein weites Spektrum von Faktoren mit ein, aber eine mathematische Formel gibt es nicht. Tatsächlich werden die vorliegenden Informationen regelmäßig unvollständig sein und dies muss jeder Entscheider berücksichtigen, wenn er selbst auf Grundlage solcher Indikatoren Entscheidungen trifft.

Simpel oder zu simpel?

Steht aber nicht zu befürchten, dass „normale Menschen" – also diejenigen, die vorrangig über einfache Indikatoren angeprochen, sensibilisiert oder gewarnt werden sollen – aufgrund der „normalen" Rot-Grün-Logik falsche Schlüsse ziehen und entweder übermäßig beruhigt oder übermäßig beunruhigt agieren?

Für alle irritierend ist auf jeden Fall die *Vielfalt* der Indikatoren: „Jeder" Anti-Viren-Software-Hersteller und Anbieter von Managed-Security-Services hat heute einen Indikator auf seiner Web-Site anzubieten. Und diese Warnungen unterscheiden sich nicht nur in der Definition, sondern auch in den konkreten Werten: Würde man sich die Mühe machen, in einem „Security-Dashboard" alle verfügbaren Indikatoren nebeneinander zu stellen, ergäbe sich ein buntes, wenn nicht sogar chaotisches Bild. Am Tag, an dem dieser Artikel entsteht, zeigt beispielsweise die ISC-Ampel grünstes Grün, während „Deutschland sicher im Netz" mit Orange die Nutzer vor akuten Bedrohungen warnt, deren Verbreitung oder Schadensausmaß „signifikant" sind. Eigentlich alles wie immer! ■

Die <kes>-Rubrik *CERT News* berichtet über aktuelle Entwicklungen aus dem Umfeld von Computer Emergency bzw. Security Incident Response Teams (CERTs/CSIRTs). Betreuer dieser Kolumne ist **Klaus-Peter Kossakowski** (www.kossakowski.de), der bereits ab 1992 mit dem Aufbau des ersten CERTs in Deutschland betraut und bis Juni 2005 Vorsitzender des internationalen Dachverbands FIRST (www.first.org) war.