der Transportebene nach unten hin ab. Sie ist zu allen SINA L2 Box S Geräten kompatibel. Wesentlicher Unterschied zu den anderen Boxen ist der Formfaktor: Die SINA L2 Box S 50M compact findet mit einer Größe von nur 210 x 220 x 42 mm bequem auf jedem Schreibtisch Platz.

Das Tischgerät benötigt keinen Lüfter, arbeitet daher geräuschlos und eignet sich für den Einsatz in Umgebungen ohne besonderen Anspruch an Schall- und Klimaschutz, also im Büro oder im heimischen Arbeitszimmer.

Für den alternativen Einsatz im Serverschrank sind entsprechende Halterungen erhältlich, die in einem 19 Zoll Rack zwei Geräte nebeneinander aufnehmen können.

Die Verschlüsselung der Informationen erfolgt im Gerät hardwarebasiert - die Authentisierung über einen externen Smartcard Leser. Die in Deutschland produzierte SINA L2 Box S 50M compact lässt sich entweder über eine SINA Management Installation oder direkt am Gerät konfigurieren und ist ab sofort verfügbar.

ENISA: Top Cyber-Bedrohungen im Threat-Landscape-Report 2013

Die „Internet-Sicherheits"-Agentur der Europäischen Union, ENISA, hat den jährlichen Threat-Landscape-Report 2013 veranlasst, in dem mehr als 200 öffentliche Reports und Artikel analysiert wurden. Dieser stellt folgende Fragen: Was waren die Top Cyber-Bedrohungen 2013? Wer sind die Gegner? Was sind die wichtigen Trends bei Cyber-Bedrohungen im digitalen Ecosystem? Zu den entscheidenden Ergebnissen gehören, dass Cyber-Bedrohungen nun auch im Mobilbereich zu finden sind und dass die Annahme von einfachen Sicherheitsbestimmungen durch Endnutzer die Anzahl der Cyber-Vorfälle um 50% reduzieren würde. Die Studie wurde im Zusammenhang mit dem von der Agentur organisierten jährlichen Zusammentreffen hochrangiger Mitglieder in Brüssel am 11. Dezember 2013 veröffentlicht.

Der ENISA Threat-Landscape-Report präsentiert die aktuellen Cyber-Bedrohungen 2013 und identifiziert Trends. Im Jahr 2013 haben erhebliche Änderungen und herausragende Erfolge ihren Einfluss im Cyber Bedrohungsumfeld hinterlassen. Sowohl positive als auch negative Entwicklungen haben das Bedrohungsumfeld 2013 geprägt. Insbesondere:

Negative Trends 2013:

- Bedrohungsagenten haben die Feinheit ihrer Attacken und ihrer Werkzeuge verbessert.
- Es ist klar, dass Cyberaktivitäten nicht nur Gegenstand für eine Hand voll von Nationen ist. In der Tat haben verschiedene Staaten die Kapazität entwickelt, sowohl Regierungsziele als auch private Nutzer zu unterwandern.
- Cyber-Bedrohungen sind nun auch im Mobilbereich zu finden: Angriffsstrukturen und –werkzeuge, die PCs im Visier haben, wurden vor wenigen Jahren entwickelt und sind nun in das mobile Ecosystem gewandert.
- Zwei neue digitale Schlachtfelder haben sich entwickelt: Big Data und das Internet der Dinge.

Positive Entwicklungen bei den Cyber Bedrohungs-Trends 2013 sind:

- Einige beeindruckende Erfolge beim Gesetzesvollzug: die Polizei hat eine kriminelle Bande verhaftet, die für einen Polizeivirus verantwortlich ist. Der Betreiber der Internetseite „Silk Road" als auch die Entwickler und Betreiber von „Blackhole", dem bekanntesten Ausbeutungs-Bausatz, wurden ebenfalls festgenommen.
- Eine Zunahme der Qualität und der Anzahl der Reports und der Daten bezüglich Cyber-Bedrohungen.
- Lieferanten haben an Schnelligkeit bei der Absicherung ihrer Produkte zugelegt .

Eine Tabelle der aktuellen Top Bedrohungen und Bedrohungs-Trends zeigt die folgenden Top 3 Bedrohungen auf:

1. Drive-by-Downloads,
2. Worms/Trojaner und
3. Codeinfizierungen.

Offene Themen, die identifiziert wurden:

- Die Endnutzer besitzen noch zu wenig Hintergrundwissen und müssen daher aktiv involviert werden. Die Annahme einfacher Sicherheitsmaßnahmen durch Endnutzer würde die Anzahl von Cybervorfällen weltweit um 50% reduzieren!
- Eine Vielzahl von Akteuren arbeiten an überschneidenden Themen und Bedrohungsinformationen sowie –analysen. Eine weiterführende Koordination der Informationssammlung, Analyse, Beurteilung und Bestätigung unter den involvierten Parteien ist nötig.
- Die Wichtigkeit der erhöhten Schnelligkeit bei Bedrohungseinstufungen und deren Verbreitung, durch die Reduzierung von Erkennungs- und Bewertungszyklen.

Der Report steht hier zur Verfügung: *https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats*

TeleTrusT: Koalitionsvertrag ist ermutigendes Signal für die deutsche IT-Sicherheitsbranche

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) begrüßt zentrale Festlegungen des CDU/CSU/SPD-Koalitionsvertrages zur IT-Sicherheit. Die kommende Legislaturperiode bietet die Chance, verlorenes Terrain in der IT-Sicherheitstechnologie wiederzugewinnen und Deutschland im internationalen Kontext in eine wegweisende Position zu bringen.

TeleTrusT befürwortet insbesondere die Punkte:

- Ausbau der Internet-Infrastruktur Deutschlands und Europas als Vertrauensraum;
- Eintreten für eine europäische Cybersicherheitsstrategie;
- Maßnahmen zur Rückgewinnung technologischer Souveränität;
- Entwicklung vertrauenswürdiger IT- und Netz-Infrastruktur einschließlich Entwicklung sicherer Soft- und Hardware und sicherer Cloud-Technologie;
- Schaffung eines IT-Sicherheitsgesetzes mit verbindlichen Mindestanforderungen für kritische Infrastrukturen;
- Pflicht, „erhebliche IT-Sicherheitsvorfälle" zu melden;
- Verpflichtung der Bundesbehörden, 10% ihres IT-Budgets für Systemsicherheit zu verwenden;