IT-Systemhaus ist gerüstet

"BWI kann alles, wofür sie beauftragt wird"

(BS/sp) "Gute Digitalisierung kann nicht mit einem Verteilungskampf, sondern nur in einem partnerschaftlichen Ökosystem gelingen", sagte Martin Kaloudis, CEO der BWI GmbH, auf der Berlin Security Conference (BSC). Kaloudis ist mit dem Digitalisierungsprozess bisher nicht zufrieden.

Schuld daran seien vor allem die Vorgängerorganisationen gewesen, erklärte *Kaloudis*: "Der Vergleich mit der Digitalisierungsfähigkeit der US-Army hinkt, die sind da schon wesentlich weiter." Besonders stolz sei er aber auf die Projektmanagementverantwortung: "Das ist die absolute Kernkompetenz der BWI", erklärte *Kaloudis*. Um weiter auf dem Markt wettbewerbsfähig zu bleiben, möchte das Systemhaus weiter mit Partnern wachsen und die Digitalisierungsprojekte vorantreiben: "Einige Entwicklungen haben wir auch Corona zu verdanken, zum Beispiel Mobil Clients für die Bundeswehr. "Vor der Pandemie haben wir die aufwändig beantragen müssen und nur eine gewisse Anzahl genehmigt bekommen. Heute gibt es dafür keine Beschränkungen mehr", so *Kaloudis*.

Generalleutnant Frank Leidenberger erklärt auf der BSC die digitale Zukunftsausrichtung des BWI. Foto: BS/Paul Schubert

Ein weiteres gelungenes Projekt sei der BW-Messenger: "Etwa 60.000 Soldat(inn)en besitzen nun ein sicheres Chat-Programm, mit dem sie verschlüsselt auf privaten oder dienstlichen Endgeräten kommunizieren können", erklärte *Katrin Hahn*, CRO der BWI GmbH. Die ortsunabhängige Kommunikation sei kein "Nice-to-have" mehr, sondern nötig, um zukunftsfähig, schnell und flexibel zu sein, so die Geschäftsführerin: "Die IT ist immer im Fluss und mittlerweile kämpft die Bundeswehr vor allem auf einem digitalen Gefechtsfeld."

Rüstungsfirmen würden dabei den Wert der IT trotzdem noch unterschätzen: "Teilweise denken die sich, dass das bisschen IT auch nebenher betrieben werden kann", sagte Generalleutnant *Frank Leidenberger*, CDO der BWI GmbH. "Die IT soll lösungsorientierter arbeiten und nicht technische Hardware von A nach B schaffen. Das ist der völlig falsche Ansatz. Wir müssen das alles standortunabhängig machen", so *Leidenberger*. Im Endeffekt sei die BWI zu allem fähig: "Eigentlich kann die BWI alles machen, wofür sie beauftragt wird", so der General.

Was heißt unabhängig?

Koalitionspartner wollen BSI neu aufstellen

(BS/Paul Schubert) Im Koalitionsvertrag der Ampelparteien wollen die Koalitionäre vor allem auf Open Source und Digitale Souveränität setzen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) soll unabhängiger aufgestellt werden, das Mittel der aktiven Cyber-Abwehr – Hack-back genannt – wird weiter abgelehnt. Reicht das, um den Gefahren aus dem Netz in dieser Legislaturperiode zu begegnen?

In einem sind sich Netz- und Digitalexpert(inn)en beim Thema IT-Sicherheit schon seit einigen Jahren einig: Das Thema muss zur Chefsache gemacht werden. Beim Blick auf das Koalitionspapier, welches im November veröffentlicht wurde, drängt sich die Frage auf, inwiefern die SPD, die Grünen und die FDP diesem Leitspruch auch folgen werden. Insgesamt 177 Seiten umfasst das Papier der Ampelparteien, die IT-Sicherheit nimmt – zusammen mit dem Thema "Digitale Bürgerrechte" – dabei knapp eine halbe Seite ein. Zwar taucht das Schlagwort "IT-Sicherheit" im Dokument noch an der einen oder anderen Stelle auf, dennoch kann die Frage gestellt werden, ob das einer modernen, digital-affinen Welt noch gerecht wird.

Im neuen Koalitionsvertrag findet sich eine halbe Seite zur IT-Sicherheit. Reichlich wenig, wenngleich die wichtigen Themen wie Open Source, Neuausrichtung des BSI und sichere Kommunikation angesprochen werden. Aber reicht das? Foto: BS/Sozavisimos, pixabay.com

In die richtige Richtung

Im Grundsatz werden die richtigen Themen angesprochen. Die Parteien versprechen ein Recht auf Verschlüsselung und ein effektives Schwachstellenmanagement. Hiermit ist vor allem die rechtzeitige Schließung von Sicherheitslücken gemeint. Hier zeichnet sich eine Trendwende ab: White-Hat-Hacking soll legal werden: "Das Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren, z. B. in der IT-Sicherheitsforschung, soll legal durchführbar sein", heißt es im Papier. Dies würde bedeuten, dass "ethische Hacker/-innen" zukünftig nicht mehr strafrechtlich belangt werden dürften. Ethische Hacker/-innen sind Personen, welche IT-Sicherheitsmängel in IT-Infrastrukturen an die entsprechenden Stellen melden und nicht zu ihrem eigenen Vorteil nutzen. Das prominenteste Beispiel aus der jüngsten Zeit ist die IT-Forscherin *Lilith Wittmann*, welche eine Sicherheitslücke in der CDU-Connect-App entdeckt hatte und daraufhin von den Christdemokraten angezeigt wurde. Es kann damit gerechnet werden, dass der sogenannte "Hackerparagraf" 202c – welcher die Anzeige erst möglich gemacht hat – im Strafgesetzbuch modifiziert werden wird. Weiterhin lobenswert sind die geforderten Vorgaben von Security-by-Design/Default und die Haftung von Herstellern, die fahrlässig IT-Sicherheitslücken in ihren Produkten verursachen.

Des Weiteren möchten die Ampelparteien auch den Weg der digitalen Souveränität weiter beschreiten. Das gilt auch für den Fokus auf offene Standards, die Schaffung europäischer Ökosysteme beim Thema 5G oder Künstliche Intelligenz und die Verpflichtung einer durchgängigen Ende-zu-Ende-Verschlüsselung auf allen Kommunikationskanälen. Auch das Dauerdiskussionsthema zur Nutzung von Open Source ist im Papier präsent: Mehr Nutzung von Open-Source-Software, weniger Fokus auf proprietäre Software, heißt es im Koalitionsvertrag. Fördermöglichkeiten sollen vor allem für DSGVO-konforme Datenverarbeitung und den Einsatz digitaler Technologien für kleine und mittlere Unternehmen möglich gemacht werden.

Mehr Unabhängigkeit für das BSI

Interessant ist die zukünftige Rolle des BSI. So soll das Bundesamt zukünftig "unabhängiger aufgestellt und als zentrale Stelle im Bereich IT-Sicherheit ausgebaut werden." In welcher Form diese Unabhängigkeit hergestellt werden soll, erwähnt das Papier nicht. Des Weiteren stellen die drei Parteien klar, dass das Offenhalten von Sicherheitslücken weiterhin abgelehnt wird und verpflichten die Cyber-Sicherheitsbehörde des Bundes dazu, die Schließung von Sicherheitslücken schnellstmöglich durchzuführen. Auch der Passus, dass "nicht vertrauenswürdige Unternehmen" nicht am Ausbau von Kritischen Infrastruktur (KRITIS) beteiligt werden sollen, ist vage formuliert. Gut möglich, dass damit die Vergabe des 5G-Ausbaus des chinesische Unternehmen Huawei weiter ausgeschlossen werden wird. Nicht überraschend ist die Ablehnung von aktiver Cyber-Abwehr. Bis auf die Christdemokraten lehnen dieses Verfahren alle demokratischen Parteien im Bundestag seit einiger Zeit ab. Ähnliches soll für die Uploadfilter gelten. Hier sehen die Koalitionspartner die Informations- und Meinungsfreiheit gefährdet und lehnen eine verpflichtende gesetzliche Grundlage für diese Art von Software ab.

Auch die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZiTis) wird im Koalitionspapier scharf in den Blick genommen. Allerdings verweisen die Koalitionäre hier vor allem auf gesetzliche Grundlagen mit klaren Zuständigkeiten und "garantieren die lückenlose Kontrolle durch Parlamente und Datenschutzaufsichtsbehörden". Eine ähnliche Wahrung der Grundrechte soll durch die strenge Kontrolle von Online-Durchsuchungen ermöglicht werden: "Solange der Schutz des Kernbereichs privater Lebensgestaltung nicht sichergestellt ist, muss ihr Einsatz unterbleiben", heißt es im Koalitionsvertrag.

Schlussendlich spricht das Papier viele wichtige Punkte im Bereich der IT-Sicherheit an, bleibt bei den genauen Umsetzungsmöglichkeiten aber vage. Aber für die Präzisierung haben die neu gewählten Volksvertreter /-innen nun genug Zeit.

BSI-zugelassene VPN-Software für VS-NfD

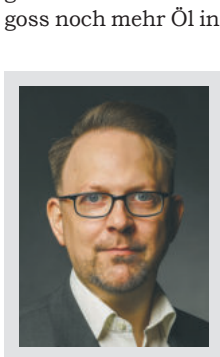
Der mobile Arbeitsplatz heute und in Zukunft

(BS) Die IT-Welt dreht sich bekanntermaßen besonders schnell. In den letzten zehn Jahren gab es viele verschiedene Entwicklungen im Bereich von Hard- und Software zur sicheren Datenkommunikation der Geheimhaltungsstufe VS-NfD (Verschlusssachen – Nur für den Dienstgebrauch).

Erhielten anfangs noch Produkte nach gewissen Kriterien eine Einsatzempfehlung des Bundesamts für Sicherheit in der Informationstechnik (BSI), wurde ab 2012 eine BSI-Zulassung durch die höhere Bedrohungslage zur Vorgabe. Es entstanden Hardware-Lösungen oder Produkte basierend auf Virtualisierung, da Windows als Betriebssystem als unsicher galt. An letzterem Sachverhalt hat sich bis heute nichts verändert.

VPN für VS-NfD: Hardware ist Vergangenheit

Seit 2019 kam es aufgrund der schlechten Usability und Skalierbarkeit von Hardware zu einem Umdenken. Die prekäre Situation in der Corona-Pandemie durch Hardware-Lieferschwierigkeiten und den plötzlich erhöhten Homeoffice-Bedarf auch bei Bedarfsträgern, Behörden und der geheimschutzbetreuten Wirtschaft goss noch mehr Öl ins Feuer. Als Vorreiter konnte NCP bereits im Juli 2020 mit dem NCP VS GovNet Connector die erste Softwarelösung mit Freigabeempfehlung des BSI für Endgeräte mit Standard-Windows-10 auf den Markt bringen. Zudem ist der Anbieter seit April 2021 "Qualifizierter Hersteller für das Qualifizierte VS-NfD-Zulassungsverfahren im Sinne des Bundesamtes für Sicherheit in der Informationstechnik" und kann daher innovativ und trotzdem schnell auf Marktanforderungen reagieren. Auf Hardware oder Hardware-Abhängigkeit setzt man beim Nürnberger Software-Spezialisten aus guten Gründen nicht mehr.



Benjamin Isak ist Director Sales Public & Defence bei NCP. Foto: BS/privat

Aktuelle Einsatzmöglichkeiten

Die Version 2.0 des NCP VS GovNet Connectors besitzt seit dem 14.05.2021 eine BSI-Zulassung für die Geheimhaltungsstufen "VS-NfD", "RESTREINT UE/EU RESTRICTED" und "NATO RESTRICTED". Durch ihre Leistungsfähigkeit, Skalierbarkeit und den ausgereiften Funktionsumfang unterscheidet sich die Lösung im Einsatzverbund mit den zentralen NCP-Software-Komponenten deutlich von Produkten anderer Hersteller auf dem Markt. Roll-Out, Inbetriebnahme, Softwareupdate und Administration der gesamten "NCP VS GovNet" Lösung" erfolgen komfortabel über eine zentrale Management-Komponente, das NCP Secure Enterprise Management (SEM). Der für VS-NfD zugelassene "NCP Secure VPN GovNet"-Server schließt den Kreis der Gesamtlösung. Im Zusammenspiel mit den hoch leistungsfähigen, zentralen Softwarekomponenten können Nutzerzahlen jenseits der 100.000 problemlos abgebildet werden. Die Verwendung von Standard-Hardware in Verbindung mit einem Standard-Windows-10-Betriebssystem eröffnet Anwendern ganz neue Möglichkeiten und erlaubt maximale Flexibilität. Ein Integritätsdienst sorgt in gleichem Maße für erhöhte Sicherheit wie starke Authentisierungsmöglichkeiten und weitere Sicherheitsfunktionen z. B. im Rahmen von Network Access Control und Endpoint Policy Checks. Über sichere und zugleich komfortable Möglichkeiten der Administration wie z.B. das zentrale Rechte- und Konfigurationsmanagement oder "Quality of Service"-Unterstützung freuen sich IT-Verantwortliche. Verschiedene anwender- bzw. bedarfsgerechte Lizenzmodelle, wie z. B. das Pay-per-Use-Lizenzmodell, runden die VS-NfD-Software-Lösung ab.

Sichere Datenkommunikation im Digitalen ist schwer zu erreichen. Mit dem "NCP VS GovNet Connectors"-Version 2.0 bietet das Unternehmen Sicherheitslösungen für diverse Geheimhaltungsstufen. Foto: BS/Sergey Nivens, stock.adobe.com

Sichere Hotspot-Anmeldung & Friendly Net Detection

Diese und weitere Vorteile orientieren sich durch jahrelange Erfahrung und Zusammenarbeit ganz eng am tatsächlichen Praxisbedarf. Die Lösung weiterer für die Bedarfsträger relevanter Probleme folgen bei der Zulassung der nächsten Produktversion 2.10 des NCP VS GovNet Connectors bereits im Dezember. Im Fokus stehen hier insbesondere die sichere Nutzung öffentlicher Hotspots und eine Friendly Net Detection (FND). Die übliche Anmeldung über eine Website des Hotspot-Betreibers mit einer Kommunikation am VPN-Tunnel vorbei ist im Behörden- und Business-Umfeld meist nicht gestattet, weswegen die Nutzung öffentlicher Hotspots quasi unmöglich wird. Wählt ein Anwender der NCP-Lösung einen Hotspot aus, baut der VS GovNet Connector automatisch die Verbindung zum Unternehmensnetz auf. In den meisten Fällen ist ein Internetzugang nicht ohne Anmeldung möglich, sodass der Client zu diesem Zweck aus Sicherheitsgründen einen funktionsreduzierten Webbrowser startet. So können Anwender auf sichere Weise einen öffentlichen Hotspot nutzen, ohne an den Sicherheitseinstellungen etwas ändern zu müssen.

Das Feature "Friendly Net Detection (FND)" erkennt zertifikatsbasiert, ob sich der Anwender in einem sicheren oder unsicheren Netz befindet und aktiviert die entsprechenden Firewall-Regeln. Im sicheren Netzwerk kann der VPN-Verbindungsaufbau somit unterbunden werden, damit beispielsweise administrative Zugriffe auf das Endgerät gestattet sind, während dies im unsicheren Netz nicht erlaubt ist. Im Gegensatz zu herkömmlichen Firewalls ist die des NCP VS GovNet Connectors bereits beim Systemstart aktiv. Voraussetzung für die Verwendung des FND-Features ist der Einsatz des "NCP Friendly Net Detection"-Servers ab Version 4.0.

Was kann VPN-Software für VS-NfD in Zukunft?

Die Vision einer leistungsstarken, zentral administrierbaren NCP-Softwarelösung für VS-NfD wird in den kommenden Monaten auch Punkte wie REST-API, eine Single-Sign-on-Lösung, Client-Software für weitere Betriebssystem-Plattformen und zusätzliche Komfortfunktionen bei der Installation und Konfiguration großer Nutzerzahlen beinhalten. Ziel ist es, Kunden hochskalierbar, hochsicher und gleichzeitig maximal flexibel auch für die Datenkommunikation nach "VS-NfD" auszustatten. Auch VS-Arbeitsplätze müssen remote für Homeoffice und mobiles Arbeiten bei großen Nutzerzahlen gut administrierbar sein. Managed-Service-Betreiber und Landesrechenzentren können einzelne Mandanten über eine zentrale Plattform sicher und voneinander getrennt betreuen, auch wenn Kunden einen Mischbetrieb aus VS-NfD und normalen Nutzern fahren. Denn besonders mit Blick in die Zukunft ist es essenziell, dass Anwender in den sensiblen Bereichen – im Geheimschutz sowie in der Verteidigung – mit adäquaten und innovativsten Lösungen ausgerüstet sind. Dies ist die Grundlage, um die wichtigen hoheitlichen Aufgaben zu jeder Zeit und unterbrechungsfrei durchführen zu können.

Informieren Sie sich über die Einsatzmöglichkeiten und Funktionen unter www.ncp-e.com.