Interview

mit Dr. Enno Littmann,
Geschäftsführer IHSE GmbH

Herr Dr. Littmann, Sie sind zum ersten Mal mit der Firma IHSE in unserem cpmFORUM vertreten. Das militärische Umfeld ist für Ihr Unternehmen aber keineswegs neu. Können Sie uns die Firma IHSE kurz vorstellen?

IHSE ist ein Entwickler und Hersteller von KVM-Hardware. KVM steht für Keyboard-Video-Mouse, die üblichen Ein- und Ausgabegeräte am Arbeitsplatz: Tastatur, Monitor und Maus. Das Unternehmen wurde 1984 gegründet.

Laienhaft ausgedrückt, stellen wir Senderboxen her, die in die Tastatur-, Monitor- und Maus-Buchsen einer Computer-CPU eingesteckt werden und diese Signale transkodieren, um sie über dedizierte Cat-X- oder Glasfaserkabel an eine unserer Empfängerboxen am Bedienpult zu übertragen. Diese dekodieren das Signal und sind an einen Bildschirm sowie Tastatur und Maus angeschlossen.

Die Entfernung dieser Verkabelung kann viele Meter (oder gar Kilometer) betragen, aber dank des fortschrittlichen Designs mit niedriger Latenz ist die Benutzererfahrung die gleiche, als ob der Computer unter Ihrem Schreibtisch stünde – anders als bei den Standard-Remote-Desktop-Protokollen.

Darüber hinaus stellen wir KVM-Matrizen für sicheres Umschalten her, die sich zwischen den Computern und den Benutzern befinden. Vereinfacht ausgedrückt handelt es sich dabei um eine Art Schalttafel, über die viele angeschlossene Computer mit vielen Bedienpulten oder Video-Walls in einer Leitstelle oder Kommandozentrale verbunden werden können – und das alles mit geringster Latenz, höchster Qualität und größter Sicherheit.

Der Vorteil dabei ist, dass die Computer nicht mehr unter den Schreibtischen in der Leitstelle stehen, sondern in sicheren Serverräumen untergebracht sind. Das verhindert die Lärm- und Hitzebelästigung im Raum und verringert das Risiko eines unbefugten Zugriffs, während gleichzeitig eine einfache gemeinsame Nutzung (Sharing) oder Zusammenarbeit an einem oder mehreren Computern ermöglicht wird.

Während unsere Produkte in der Vergangenheit für den industriellen und kommerziellen Markt entwickelt wurden, gab es immer eine stetige Nachfrage aus der Verteidigungsindustrie, die die Funktionalität und die einfache Integration unserer hochsicheren Systeme in ihre Projekte zu schätzen wussten. In jüngster Zeit hat dies dazu geführt, dass wir eine spezielle Produktlinie für den NATO-Verteidigungsmarkt mit NIAP PP 4.0-Zertifizierung namens IHSE Secure entwickelt haben.

Datensicherheit ist eines der wichtigsten Themen der letzten Zeit im Bereich der kritischen Infrastrukturen und im militärischen Umfeld. Inwieweit schützen Ihre Produkte vor internen und externen Angriffen auf hochsensible Daten?

IHSE befasst sich sehr stark mit internen Angriffen oder mit dem, was wir „Insider Threat" nennen. Wir beugen der Gefahr vor, dass jemand, der auf dem Gelände oder in der Leitstelle arbeitet und Zugang zu sensiblen Daten hat, Geheimnisse für unsere Gegner stiehlt oder unsere Systeme beschädigt.

Denken Sie nur an Edward Snowden oder Chelsea Manning, die mit Hilfe von USB-Sticks, die in Computer eingesteckt wurden, sensible Daten heruntergeladen haben, oder an all die anderen, die noch entdeckt werden müssen und deren Methoden sich weiterentwickeln und immer raffinierter werden.

Natürlich könnten wir einfach alle Computer sperren, aber in einem sich entwickelnden Verteidigungsumfeld müssen die Mitarbeiter in der Lage sein, Systeme, Informationen und Daten gemeinsam zu nutzen, um Situationen zu analysieren und schnelle Entscheidungen zu treffen.

Eine moderne Kommandozentrale empfängt während eines Großereignisses immer mehr Videoinformationen und Nachrichtenströme (oft von einer Koalition von Verbündeten). Diese werden laufend eingespielt, um ein umfassenderes Lagebild zu vermitteln und eine sofortige Aktualisierung der getroffenen Maßnahmen zu ermöglichen. All diese Daten sind live, höchst vertraulich und potenziell dem Risiko des Diebstahls oder Missbrauchs ausgesetzt. In gemischten Umgebungen, in denen Bereiche mit unterschiedlichen Vertraulichkeitsstufen (Multi-Class) kombiniert werden, kommt noch mehr Komplexität hinzu.

Das IHSE KVM-System überträgt lediglich Pixelpakete von der CPU, um die Computerbilder anzuzeigen. Vom Benutzerarbeitsplatz aus ist der Datentransport streng auf Tastatur- und Maussignale zur Steuerung der CPU beschränkt. Alle Computersysteme, ihre Festplatten, USB-Anschlüsse und Daten werden von den Mitarbeitern ferngehalten und in einer gesicherten Einrichtung unter Verschluss gehalten, zu der nur Systemmanager mit den höchsten Sicherheitsüberprüfungen, Prozessen und Verfahren Zugang haben.

Welche Zertifizierungen haben Ihre Produkte?

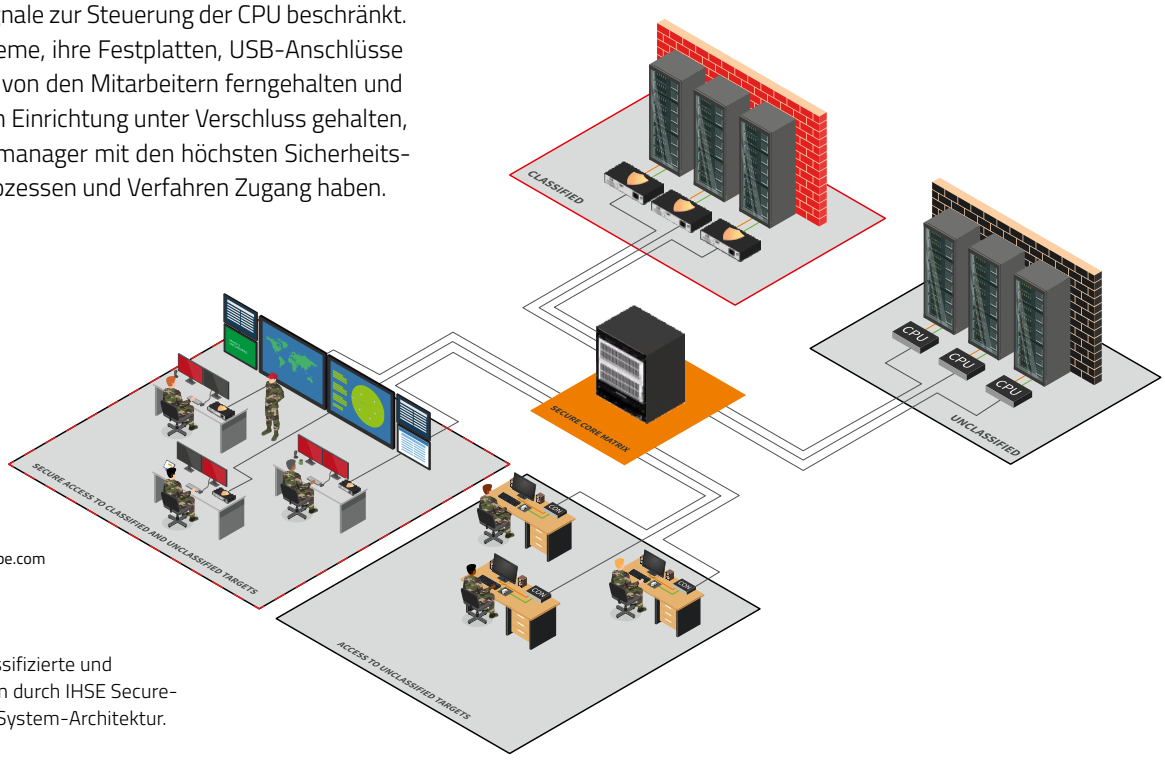
IHSE Secure ist eine Produktreihe, die wir als Reaktion auf die Bedürfnisse unserer Kunden aus den Bereichen Verteidigung und kritische Infrastrukturen entwickelt haben, die der Meinung sind, dass das Risiko von Spionage und Schäden an Systemen gestiegen ist. IHSE verfolgt einen proaktiven Ansatz auf dem Markt für Cybersicherheit im Allgemeinen.

Die ersten IHSE Secure-Produkte haben die Common Criteria NIAP PP4.0-Zertifizierung für die gemeinsame Nutzung von Peripheriegeräten unterschiedlicher Vertraulichkeitsstufen erhalten, und wir erwarten die Common Criteria EAL4-Zertifizierung in Kürze, zu der in Zukunft weitere Produkte für das Secure-Portfolio hinzukommen werden.

Das klingt sehr aufregend. Bei der Vernetzung vieler verschiedener Systeme im Kampfeinsatz denke ich auch an eine Vielzahl von Datenpaketen mit extremen Datenmengen. Gerade für die Bildauswertung ist eine manipulationssichere Datenübertragung, auch in Echtzeit, wichtig. Stellt dies eine Herausforderung für Ihre Produkte dar?

Alle diese Systeme übertragen viele Petabytes an Daten, und es gibt eine Art „Informationswettlauf", um eine Informationsüberlegenheit gegenüber unseren Gegnern zu erreichen und gleichzeitig ein hohes Maß an Informationssicherheit zu gewährleisten.

Diese beiden Erfordernisse konkurrieren eindeutig miteinander, und eine weitere Komplikation besteht darin, dass sich die Computer der Einsatzkräfte in klassifizierten und nicht klassifizierten Netzen befinden können (oder in Netzen mehrerer Vertraulichkeitsstufen gemäß den NATO-Klassifizierungen für die Informationssicherheit). Eine gute Informationssicherungspraxis verlangt, dass Daten von einer Netzklasse nicht in die andere gelangen können und dass



▲ Foto: Framestock / stock.adobe.com

◀ Dr. Enno Littmann.
Foto: IHSE GmbH

▶ Sicherer Zugriff auf klassifizierte und nicht-klassifizierte Quellen durch IHSE Secure-Produkte innerhalb einer System-Architektur.
Grafik: IHSE GmbH

keine Möglichkeit besteht, von einem nichtklassifizierten Netz auf klassifizierte Informationen zuzugreifen.

IHSE bietet eine Lösung, bei der alle Mitarbeiter, die in einer sich schnell entwickelnden Situation sofortige Informationen benötigen, die Möglichkeit haben, diese Systeme zu nutzen und mit ihnen zu interagieren. Gleichzeitig verhindert das System, dass die Benutzer Daten mitnehmen oder sie durch Einschleusen von Schadsoftware beschädigen können.

Um das sich ständig weiterentwickelnde Manipulationsrisiko zu mindern, hat IHSE die neue Produktlinie IHSE Secure mit NIAP PP 4.0- und EAL4-Zertifizierung entwickelt.

Gibt es bereits Lösungen von anderen Herstellern? Wenn ja, wie unterscheidet sich Ihr Ansatz?

Es gibt eine große Auswahl an Desktop-Switching-Produkten von anderen Herstellern. Einige der Hersteller produzieren Multi-Class-Desktop-Switches, bei denen die Tastatur-, Monitor- und Mauskabel lokal am Desktop angeschlossen sind, wo sie unserer Meinung nach anfällig für Angriffe sind. Unser IHSE KVM-System verlagert alle diese Schnittstellen zurück in den sicheren Serverraum.

Ein wesentlicher Unterschied zwischen IHSE und anderen KVM-Systemen besteht darin, dass wir die Tastatur-, Monitor- und Mausschnittstellen hinter NIAP PP4.0-Datenisolatoren (Dioden) abschirmen. Dies bietet den Schutz von einem Ende zum anderen Ende für alle Datenströme, die an den Benutzerarbeitsplatz geliefert werden – unabhängig davon, ob eine IHSE KVM-Matrix dazwischengeschaltet ist oder nicht. Nach unserem Kenntnisstand schirmt kein anderer KVM-Hersteller seine Extender in demselben Maße ab wie IHSE.

Unser Ansatz geht davon aus, dass das Hauptrisiko auf der Benutzer- und Computerseite des KVM-Systems liegt, da hier die Schnittstellen offener Standard sind, zudem oft physisch offen liegen und generisch sind. Beispielsweise ist die Videoschnittstelle des Monitors in der Regel bidirektional, um EDID-Informationen zurück an den Computer zu leiten. Das stellt eine Angriffsmöglichkeit dar, indem ein Gefährder über den Rückkanal des Monitors Schadsoftware in den Computer einschleusen könnte.

IHSE Secure-Produkte verfügen über NIAP PP4.0-zertifizierte Isolatoren, die in die Extender-Endpunkte integriert sind und bidirektionale Datenflüsse verhindern, aber auch eine Reihe von weitaus raffinierteren Angriffsvektoren abwehren, die auf die Audio-, Tastatur- und Mausschnittstellen abzielen.

Digitale Umgebungen sind einem ständigen Wandel unterworfen. Wie stellt Ihr Unternehmen eine zukunftssichere Nutzung sicher und inwieweit können Anwender alle Lösungen Ihres Portfolios abdecken?

Diese Frage hat zwei Seiten:

Die erste ist, dass unsere Extender-Endpunkte auf der CPU-Seite und auf der Anwenderseite mit den Tastatur-/Monitor-/Mausschnittstellen verbunden sind, und diese haben sich im Laufe der Jahre verändert. Denken Sie nur an die Videoschnittstelle, die sich von einfachem VGA zu DisplayPort 1.4 entwickelt hat. IHSE hat dabei jede neue Schnittstelle kontinuierlich unterstützt, sobald sie Verbreitung fand.

Der zweite Teil betrifft die Übertragungskabel für die Signale zwischen den Endpunkten. In der KVM-Welt kommt dabei eine dedizierte Verkabelung mit Cat X- oder Glasfaserpaaren von einem Ende zum anderen Ende zum Einsatz. Zudem wird eine dedizierte proprietäre Matrix oder alternativ ein TCP/IP-Ethernet-Netzwerk mit einem Standard-Netzwerk-Switch zwischengeschaltet.

Die relativen Vorzüge jedes Ansatzes würden viele Seiten in Anspruch nehmen, aber die Schaffung eines separaten Bereichs in einem bestehenden IP-Netzwerk mit angemessener Bandbreite und Sicherheit ist eine Herausforderung und erhöht die Belastung des bestehenden Netzwerks für die Informationssicherheit aufgrund der Datenmenge, die die Videoströme erzeugen, exponentiell.

Die sicheren Produkte von IHSE verwenden eine dedizierte Ende-zu-Ende-Verkabelung über eine IHSE-Matrix, da wir der Meinung sind, dass diese schneller aufgebaut werden kann und in der Lage ist, die riesigen Datenmengen problemlos zu verarbeiten.

In einer älteren Umgebung, z.B. bei der Nachrüstung von Leitstellen, besteht jedoch möglicherweise kein uneingeschränkter Zugang zur vollständigen Neuverkabelung, und hier zeigt sich die Flexibilität der IHSE-Produkte besonders anpassungsfähig.

Wir stellen eine große Auswahl an verschiedenen Sender-/Empfänger-Endpunkten mit einer Vielzahl von Videoschnittstellenoptionen her, darunter VGA, DVI, SDI, HDMI und DisplayPort, so dass wir die meisten dieser Optionen abdecken können.

Darüber hinaus überwacht unsere Matrix-Technologie die eingehenden Signale und taktet sie neu. So ist es möglich, ein Signal über einen Kabeltyp oder einen Videostandard/eine Auflösung zu empfangen und dieses Signal über einen anderen zu senden, z.B. DVI-in und DisplayPort-out.

Fotos: Gorodenkoff / stock.adobe.com

Ein weiteres Beispiel wäre eine Leitstelle mit bestehender Cat-X-Verkabelung und MediaWall, die HD-Kacheln und HD-Monitore enthält, wobei der mit einer 4K-Grafikkarte konfigurierte Quellcomputer über Glasfaser mit der Matrix verbunden ist. Dank der oben genannten Eigenschaften kann unsere KVM-Matrix die Daten problemlos über eine herkömmliche Cat-X-Verkabelung in die Leitstelle senden.

Alles in allem ist IHSE also führend auf dem KVM-Markt, wenn es um die neuesten Schnittstellen und die Integration in heterogene oder ältere Umgebungen geht, während gleichzeitig die Einhaltung der Informationssicherheit optimiert wird.

Wenn ein System aufgrund einer Störung ausfällt, welche Möglichkeiten bieten Ihre Produkte, um den sicheren Betrieb so schnell wie möglich wiederherzustellen?

IHSE-Endpunkte können mit doppelter Stromversorgung und redundantem Datenpfad spezifiziert werden. Dabei verfügt jede Extendereinheit über zwei Netzwerkanschlüsse für den primären und sekundären Betrieb. Das sekundäre Netzwerk ist ein voll funktionsfähiges Backup-Netzwerk, das bei einem Ausfall des primären Netzwerks sofort den Betrieb übernimmt.

Unsere Matrizen verfügen auch über redundante Spannungsversorgung und können mit mehreren Controllerkarten spezifiziert werden, wobei der sekundäre Controller im Falle eines Ausfalls übernimmt (redundante Matrizen).

Es gibt viele zusätzliche Gestaltungsmöglichkeiten, je nachdem, wie widerstandsfähig die spezifische Anwendung sein muss und wie vielschichtig und komplex das System sein darf.

Die Leitstellenumgebung wächst und wird immer komplexer. Was sind Ihre Zukunftspläne?

Die erforderliche Rechenleistung und die Anzahl der Systeme zur Analyse dieser komplexen, sich entwickelnden Situationen nehmen ständig zu. Immer mehr Datenströme müssen gleichzeitig analysiert werden, und es ist eine stärkere Zusammenarbeit erforderlich.

Gleichzeitig entwickeln sich auch die Angriffsvektoren für Insider-Threats weiter und eine gute Informationssicherungspraxis war nie so wichtig wie heute.

Die IHSE Secure-Produktreihe hilft Systemmanagern dabei, diese komplexen, konkurrierenden Anforderungen sowohl in neuen als auch in bestehenden Umgebungen zu erfüllen. So, wie sich die Bedrohungen weiterentwickeln, wird auch die IHSE Secure-Produktreihe wachsen, um sie zu entschärfen.

Herr Dr. Littmann, wir danken Ihnen für das Gespräch.

Das Interview führte Matthias Wunsch