Security by Design -

Grundlage unseres Produktportfolio

Vor kurzem wurde weltweit über Spionage-Chips auf Produkten von Supermicro, einem Hersteller von IT Systemkomponenten, berichtet. Trotz Zweifel an diesem Einzelfall, zeigt die Diskussion, dass **IT-Systeme und -Nutzer auf allen Ebenen angreifbar sind.**

Die steigende Komplexität und Integrationsdichte der IT-Systeme sowie unübersichtliche Lieferketten stellen ein erhebliches Risiko dar. Es ist daher erforderlich, Cybersicherheit in allen Phasen des Lebenszyklus und allen Ebenen von IT Systemen umzusetzen; also: **Security by Design.**

„*Dies ist bei infodas nicht nur ein **Grundpfeiler für die Beratung** unserer Kunden, sondern auch unser eigener **Leitgedanke bei der Entwicklung** unserer Produkte.*" sagt der Leiter Geschäftsfeldentwicklung der infodas, Marc Akkermann.

Wir führen immer eine umfassende Betrachtung möglicher Schwachstellen und Angriffsvektoren für unsere Produkte und Lieferketten durch, um damit **den höchsten Sicherheits- und Qualitätsstandards** gerecht zu werden.

Die Planung, Entwicklung und Fertigung unserer Produkte erfolgt in Deutschland. Es sind **keine Hardware-Komponenten von Supermicro verbaut und unsere Produkte verfügen über keine versteckten Zugänge**. Unsere System-Architektur ist von der Hardware über das Mikrokern-Betriebssystem bis hin zur Anwendungsschicht so aufgebaut, das selbst Schwachstellen wie SPECTRE oder MELTDOWN sich in nicht ohne Weiteres ausnutzen lassen.

Wir haben das Risiko von Standardhardware bereits früh erkannt, daher u. a. eine sichere Netzwerkkarte entwickelt. Eines ihrer zentralen Cybersicherheits-elemente ist ein nicht manipulierbarer Chip mit FPGA (Field Programmable Gate Array). Die sichere Netzwerkkarte kann sowohl im Client- als auch im Serverbereich zur Absicherung eingesetzt werden.

Security by Design -

Basis of our product portfolio

Recent global news reporting raised concerns about undisclosed spy chips embedded on products from Supermicro, a manufacturer of IT system components. Despite doubts about its validity, this case underlines that **attacks on IT systems and users can occur at all levels.**

The increasing complexity of today's IT systems and intransparent supply chains represent a significant risk. It is critical to secure all levels and stages of an IT system's lifecycle which means: **Security by Design.**

"*At infodas, this is not only a **cornerstone for advising** our clients, but also our own **guiding principle in the development** of our products.*" says Marc Akkermann, Head of Business Development at infodas.

We always conduct an extensive analysis of vulnerabilities and attack vectors for our products and supply chains **to meet the highest security and quality standards.**

Our products are designed, developed and manufactured in Germany. **None of our products use Supermicro components or non-declared backdoors**. Our system architecture design - from hardware, microkernel operating system to the application layer - even prevents exploitation resulting from vulnerabilities like SPECTRE or MELTDOWN.

Infodas always considered standard hardware components a risk and therefore developed a secure ethernet card. Among others it uses a tamper proof FPGA (Field Programmable Gate Array). The secure network card can be used to protect both clients and servers.

Köln/Cologne
06. Nov 2018