„WinGuard“ versteht sich als offene und herstellerneutrale Integrationsplattform, mit der unterschiedliche sicherheits- und gebäudetechnische sowie Kommunikationssysteme verschiedenster Hersteller in einer einheitlichen Benutzeroberfläche zusammengeführt werden. Foto: Advancis

„Die Gefahren sind sehr real“

IT-Angriffe treffen immer öfter auch Firmen der Sicherheitsbranche.

ANDREAS ALBRECHT

Im Zuge der Digitalisierung und Vernetzung lauern zunehmend ernste Gefahren aus den Bereichen Cybercrime, Hacking und Spionage. Darüber sprach PROTECTOR mit Andre Meiswinkel, COO der Advancis Software & Services GmbH.

Herr Meiswinkel, wie hoch schätzen Sie persönlich die Gefahr von IT-Angriffen auf Unternehmen der Sicherheitsbranche aktuell ein?

» **Andre Meiswinkel:** Diese Gefahr ist tatsächlich hoch und real, natürlich nicht nur für Unternehmen der Sicherheitsbranche, sondern generell. Im Fokus von Hackern stehen zunehmend Betreiber kritischer Infrastrukturen wie etwa Energie- oder Wasserversorger, Unternehmen im Transport- und Verkehrswesen, aber auch staatliche Institutionen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bestätigt, dass die Anzahl der registrierten Attacken zugenommen hat. Denken wir zum Beispiel an die Sicherheitslücke bei Whatsapp, durch welche Hacker unbemerkt Überwachungssoftware auf Smartphones installieren konnten. Verdächtigt wird ein Unternehmen, das Spionagetechnik an Regierungen verkauft. Das Ganze war aufgefallen, als jemand verdächtige Whatsapp-Anrufe auf seinem Telefon bemerkte und sich daraufhin an Sicherheitsexperten wandte. Anfang April 2019 wurde ebenfalls öffentlich bekannt, dass der Bayer-Konzern Opfer einer Cyberattacke durch die Schadsoftware „Winnti“ geworden war. Das BSI warnt daher, dass die Bedrohungslage für die deutsche Wirtschaft auf einem hohen Niveau liege. Der ehemalige FBI-Chef James Comey sagte bereits im Jahr 2014, dass es zwei Arten von Unternehmen gibt: Diejenigen, die bereits gehackt worden sind, und diejenigen, die noch nicht wissen, dass sie gehackt worden sind. Dies ist natürlich eine bewusst zum Nachdenken anregende These, jedoch empfiehlt es sich, zur Identifizierung des Risikos und zur Einleitung qualifizierter Maßnahmen spezialisierte Fachfirmen zu konsultieren. Diese empfehlen unter anderem, die IT-Infrastruktur auf den neuesten Stand zu bringen und zum Beispiel Penetrationstests durchführen zu lassen, um Sicherheitslücken zu identifizieren. Zudem können Darknet-Analysen beauftragt werden, aus denen hervorgeht, welche Informationen bereits über das Unternehmen ausgetauscht werden.

„Jedes Unternehmen ist in der Pflicht, nicht nur seine IT-Infrastruktur und das geistige Eigentum zu schützen, sondern auch Informationen und Daten von Fremdfirmen.“

Andre Meiswinkel, COO der Advancis Software & Services GmbH.

Foto: Advancis

In letzter Zeit häuften sich Meldungen über gehackte IP-Kameras. Einige Hersteller kooperieren mit IT-Sicherheits-Experten, um ihre Kameras bestmöglich abzusichern. Wie schützt Advancis seine Softwareplattform „WinGuard“?

» **Andre Meiswinkel:** „WinGuard“ versteht sich als offene und herstellerneutrale Integ-

rationsplattform, mit der unterschiedliche sicherheits- und gebäudetechnische sowie Kommunikationssysteme verschiedenster Hersteller in einer einheitlichen Benutzeroberfläche zusammengeführt werden. Somit ist der Nutzer völlig frei in der Wahl seiner „Subsysteme". Nach Bewertung der technologischen Merkmale und der Kosten kann er das für ihn optimale System einsetzen. Zusätzlich sollte er bei seiner Entscheidung natürlich auch die Sicherheitsmechanismen, über welche das System verfügt, mit in Betracht ziehen: Werden beispielsweise die Videodatenströme des Videomanagementsystems verschlüsselt oder verfügt die Zutrittskontrollanlage über Filterfunktionen entsprechend der DSGVO? Verschlüsselt das Schlüsselmanagementsystem die Kommunikation zwischen dem Transponder und den Türsensoren, um das Kopieren oder Identifizieren eines Transponders zu verhindern? Dies sind nur einige Beispiele für Maßnahmen zur Erhöhung der Cybersicherheit technischer Systeme. Unsere Aufgabe als Hersteller der Gefahren- und Gebäudemanagementplattform „WinGuard" ist es, die Netzwerkkommunikation mit den angebundenen Systemen und den Bedienplätzen sowie die Datenbanken zu verschlüsseln. Dies realisieren wir unter anderem über AES 256 (Advanced Encryption Standard), einen sogenannten Blockchiffren-Algorithmus, der auch durch das BSI in seiner Richtlinie vom Februar 2019 zur Verwendung in neuen kryptographischen Systemen empfohlen wird. Ebenfalls ist diese Verschlüsselungsmethode auch in den USA für staatliche Dokumente mit höchster Geheimhaltungsstufe zugelassen. Außerdem schützen in „WinGuard" sicher gespeicherte Signaturen alle verwendeten Dateien vor unberechtigten Manipulationen. Sollte beispielsweise ein Hacker versuchen, die Konfigurationsdatei einer Schnittstelle zu einem angebundenen System zu ändern – zum Beispiel den Befehl zur Scharf-/Unscharfschaltung an eine Einbruchmeldeanlage umzukehren, so dass sich die Anlage beim Befehl „Scharfschalten" in Realität unscharf schaltet – würde ein solcher Eingriff durch „WinGuard" blockiert werden.

Tragen Unternehmen, deren Geschäftsmodell Sicherheit ist, mehr Verantwortung für den Schutz ihrer Infrastruktur als andere?

» **Andre Meiswinkel:** Grundsätzlich ist jedes Unternehmen in der Pflicht, nicht nur seine IT-Infrastruktur und das geistige Eigentum zu schützen, sondern insbesondere auch Informationen und Daten von Fremdfirmen, etwa Produktinformationen, Kunden- und Lieferantendaten. Natürlich steht die Sicherheitsbranche im Fokus, und allein unsere Branchenbezeichnung verpflichtet alle Hersteller in besonderem Maße, was den Schutz vor Cyberangriffen angeht. In unserer digitalen Welt wird die Vernetzung einzelner Systeme vorangetrieben (Stichwort IoT und Cloud-Lösungen). Daher sind die Wirtschaft im Allgemeinen und speziell die Sicherheitsbranche gefordert, ständig neue Antworten auf aktuelle Bedrohungen zu finden.

Die Vernetzung wird weiter rasant zunehmen, gleichzeitig aber wohl auch Häufigkeit und Raffinesse von IT-Attacken. Sehen Sie vor diesem Hintergrund IoT und KI für die Sicherheitsbranche eher als Chance oder Risiko?

» **Andre Meiswinkel:** Ich sehe dies definitiv als eine Chance. Selbstverständlich birgt jede Chance auch immer ein Risiko, doch ohne mit der Zeit zu gehen, ist grundsätzlich keine Weiterentwicklung möglich. Natürlich rückt das Thema IT-Sicherheit damit generell noch stärker in den Fokus, um mögliche Risiken zu minimieren. Wir leben im Zeitalter von „Big Data": Die Datenmenge und -art nehmen stetig zu, so dass insbesondere die richtige und effektive Nutzung sowie die einfache Aufbereitung (UI & KI) der Daten unverzichtbar sind. Die Firma Advancis bietet mit ihrer Gefahren- und Gebäudemanagementplattform „WinGuard" ein geeignetes Instrument, die Datenmengen, welche von den unterschiedlichsten an die Plattform angeschlossenen Systeme erhoben und gesammelt werden, für den Nutzer optimal zu filtern und aufzubereiten. So werden eine übersichtliche Anzeige sowie eine effektive Bearbeitung ermöglicht. Wir sind uns der Verantwortung bewusst, welche der Umgang mit sensiblen Daten mit sich bringt und werden unsere Softwareplattform „WinGuard" auch in Zukunft dahingehend optimieren. ■

» **Auf der Sicherheitsexpo, München:**
Stand 3-D01

» **Advancis Software & Services GmbH:**
www.advancis.de