PRESSEMITTEILUNG

Münster, 8. Oktober 2020

Kurzfassung

Münsteraner Netzwerkspezialist nimmt Hacker ins Visier

Neuer Cyber Defense Service in der nicos Unternehmensgruppe

„Hackerangriffe sind eine reale Bedrohung und eine stetig zunehmende Gefahr, die insbesondere kleine und mittlere Unternehmen vor eine Herausforderung stellt,“ so Thomas Brosch, Vorstand der nicos AG, die sich vor über 20 Jahren auf sichere, globale Datennetze spezialisiert hat. Cyberkriminelle machen vor keiner Branche halt, sie planen immer größere und vernichtendere Coups. Dass eine Hackerattacke sogar Menschenleben kosten kann, zeigte unlängst der Angriff auf die Uniklinik Düsseldorf.

Heute geht es nicht mehr darum, ob ein Unternehmen angegriffen wird, sondern wann und wie. Genau an dieser Stelle setzt der neue Cyber Defense Service der nicos AG an, der ein komplettes Maßnahmenpaket zur Prävention, Detektion und Reaktion auf Sicherheitsvorfälle umfasst, um ebenso schnell wie effizient risikoreduzierende Maßnahmen umzusetzen.

Unabhängig davon bieten die Security Experten der nicos Cyber Defense nun ein hochprofessionelles, dreistufiges „Cyber Defense Assessment“ an. Damit erhalten Unternehmen eine objektive und individuelle Erhebung des Zustandes ihrer IT-Sicherheit hinsichtlich aktueller Angriffsmuster, eine Handlungsempfehlung für die Security-Strategie und Tipps zum Ausbau der Infrastruktur. Somit können sich Unternehmen umfassend insbesondere vor aktuellen und konkreten Angriffstechniken schützen.

187 Wörter, 1.444 Zeichen (inkl. Leerzeichen)
Abdruck frei. Auch auszugsweise.

PRESSEMITTEILUNG

Münster, 8. Oktober 2020

Langfassung

Münsteraner Netzwerkspezialist nimmt Hacker ins Visier

Neuer Cyber Defense Service in der nicos Unternehmensgruppe

Bedrohungen aus dem Cyberspace nehmen kontinuierlich zu. Mit ihnen wächst die Sorge um geschäftskritische Daten und deren Zerstörung, Manipulation oder Entwendung durch Cyberkriminelle. Doch bei Cyberangriffen geht es um weit mehr als nur den Verlust von Daten, wertvoller (Arbeits-)Zeit oder Verdienstausfall durch Stillstand in Produktionsstätten und an Arbeitsplätzen. Der gute Ruf des Unternehmens steht auf dem Spiel, einhergehend mit Imageverlust. Manche Informationen werden auch für persönliche Erpressungen oder öffentliche Bloßstellungen genutzt. Dass eine Hackerattacke sogar Menschenleben kosten kann, zeigte unlängst der Angriff auf die Uniklinik Düsseldorf.

Heute geht es nicht mehr darum, ob ein Unternehmen angegriffen wird, sondern wann und wie. „Dabei sind sich Unternehmen ihrer Schwachstellen oftmals nicht bewusst“, so Thomas Brosch, Vorstand der nicos AG, die sich vor über 20 Jahren auf sichere, globale Datennetze spezialisiert hat. Studien belegen, dass rund 20 % der Unternehmen gar nicht erfahren, ob sie Zielscheibe einer Cyberattacke geworden sind, ob ihre Daten das Unternehmen verlassen haben und im Internet kursieren. (Quelle: Radware ERT Report 2019/2020 - https://www.radware.com/getattachment/27edc6d3-3175-4e1b-9c36-6086dea550f0/rad1789_ERT_Report2019_2020_0103a.pdf)

Genau an dieser Stelle setzt der neue Cyber Defense Service der nicos AG an, der ein komplettes Maßnahmenpaket zur Prävention, Detektion und Reaktion auf Sicherheitsvorfälle umfasst, um ebenso schnell wie effizient risikoreduzierende Maßnahmen umzusetzen. „Die nicos Cyber Defense ist die Feuerwehr für die Daten unserer Kunden – dieses Bild beschreibt am besten unser Vorgehen. Sie kennen Red Adair, den weltweit berühmten Feuerwehrmann? Seine Lösch-Methode: Er entzieht dem Feuer den Sauerstoff und schließt danach das Leck. **Der bestkontrollierte Brand ist allerdings der, der gar nicht erst entsteht.** Deshalb sind im ersten Schritt präventive Massnahmen essenziell. Da aber diese erfahrungsgemäß aber

nur der erste Ansatz und nicht ausreichend sind, setzen wir unseren Fokus auf Detektion und Reaktion."

Dafür bieten die Security Experten der nicos Cyber Defense nun ein hochprofessionelles, dreistufiges „Cyber Defense Assessment" an. In Phase 1 recherchieren die Security Experten – so wie es Angreifer zunächst auch tun würden, welche Informationen über ein Unternehmen bereits im Web veröffentlicht wurden und welche Schwachstellen daraus resultieren können. Beispielsweise durch frei verfügbare Informationen, die auf ein persönliches Passwort schließen lassen. In Phase 2 folgt der Blick ins Innere: eine Art Immuncheck im Abgleich mit tatsächlich existierenden Bedrohungen, verbunden mit einem ausführlichen Erhebungsbogen zum alltäglichen Umgang in Bezug auf IT-Sicherheit. „Im Ergebnis, in Phase 3, werden das tatsächliche Sicherheitsniveau dokumentiert und unverbindlich die Maßnahmen aufgezeigt, durch die dieses erhöht werden kann," erklärt Thomas Brosch. Ziel ist es, Gefahren aufzudecken und die Ausbreitung zu verhindern, Datenlecks aufzuspüren und Risiken zu minimieren**. „Mit dem ‚Cyber Defense Assessment' erhalten unsere Kunden eine objektive und individuelle Handlungsempfehlung für ihre IT-Security-Strategie und Tipps zum Ausbau der Infrastruktur, um sich bestmöglich vor Cyberangriffen zu schützen."**

„Ein weiteres Problem ist auch die fehlende Awareness und mangelnde Sensibilisierung der Mitarbeiter," so Brosch. „Die besten technischen Maßnahmen helfen nicht, wenn die Mitarbeiter diese versehentlich oder unbewusst umgehen." Diese sind sich der immer näher rückenden Bedrohung durch Cyberangriffe häufig nicht bewusst. Dabei ist auch Security Awareness ein entscheidender Faktor – für die Sicherheit der Daten und das Business des Unternehmens.

„Hackerangriffe sind eine reale Bedrohung und eine stetig zunehmende Gefahr, die insbesondere kleine und mittlere Unternehmen vor eine Herausforderung stellt", berichtet Thomas Brosch. Cyberkriminelle machten vor keiner Branche halt. Sie planen immer größere und vernichtendere Coups. In Zeiten von Digitalisierung und zunehmender Komplexität der Datennetze sowie stetig wandelnder Netzwerkumgebung haben unternehmenseigene IT-Abteilungen vielfach nicht die erforderlichen Kapazitäten und das fachliche Know-how, um das Unternehmensnetz vor Cyberangriffen zu schützen. Hinzu kommt, dass Cyberattacken immer ausgefeilter werden. Cyberkriminelle gehen immer subtiler vor und attackieren Unternehmen gezielt. Sie senden ihren Opfern personalisierte Phishing Mails. Hacker infiltrieren Systeme, um Daten abzugreifen oder Rechner lahm zu legen. Zwar versuchen Betriebe, mit Passwortschutz, Virenscanner, Firewalls, Intrusion Detection und

Prevention Systems etc. den Angriffen Paroli zu bieten. Doch diese konventionellen Schutzmaßnahmen allein sind nicht mehr ausreichend.

Das umfangreiche Leistungsspektrum der Cyber Defense Spezialisten fasst Thomas Brosch deshalb so zusammen: „Wir sondieren die Lage, wir retten, dämmen ein und unterstützen unsere Kunden auf dem Weg in eine sichere Zukunft.“

672 Wörter, 5.191 Zeichen (inkl. Leerzeichen)
Abdruck frei. Auch auszugsweise.

PRESSEKONTAKT

Ann Neudek
Head of Corporate Responibility, Marketing & PR
Fon +49 251 986 33-5113
E-Mail: aneudek@nicos-ag.com

Andrea Braun, M. A.
Marketing Communications Manager
Fon +49 251 986 33-5111
E-Mail: abraun@nicos-ag.com

nicos AG
Münsterstr. 111
48155 Münster
www.nicos-ag.com

WEITERE INFOS

www.nicos-cdc.com

BILDMATERIAL

Hochauflösende Bilder in Druckqualität senden wir auf Anfrage gerne zu.

Thomas Brosch, Vorstand und Gründer der nicos AG

Die nicos Cyber Defense ist die Feuerwehr für die Daten ihrer Kunden

Über die nicos AG

Das inhabergeführte, eigenfinanzierte Familienunternehmen nicos AG mit Firmensitz in Münster, Westfalen, engagiert sich als Partner des Mittelstands für sichere, globale Datenkommunikation. Im Jahr 2000 gegründet, verbindet die nicos AG weltweit agierende mittelständische Unternehmen mit ihren internationalen Standorten und Produktionsstätten über globale Datennetze (WANs). Dabei übernimmt die nicos AG gemeinsam mit ihren Tochterunternehmen auf den Philippinen und in Australien alle Leistungen von der Planung über den Aufbau bis zum sicheren 24/7 Betrieb der Datennetze und die damit verbundenen Services, rund um die Uhr und an 365 Tagen im Jahr. Mit ihren Managed Services garantiert die nicos maximale Verfügbarkeit und höchst mögliche Sicherheit in der Datenkommunikation.

Mit dem Know-how aus 20 Jahren globaler Markterfahrung hat die nicos AG mehr als 4.000 Netzwerklösungen realisiert, an über 2.000 Standorten, in 130 Ländern. Heute setzen sich rund 180 Mitarbeiter, davon 160 am Standort Münster und 20 auf den Philippinen und in Australien, für die anspruchsvolle Klientel der nicos AG ein.

Über die nicos Unternehmensgruppe

Zur nicos Unternehmensgruppe gehören fünf Unternehmen. Global verteilt auf drei Kontinenten haben sich die nicos AG und ihre vier Tochterunternehmen thematisch spezialisiert.
Die nicos AG bietet alle Leistungen vom Design, der Implementierung bis hin zum 24/7 Betrieb sicherer, globaler Datennetze aus einer Hand. Die Netzwerkspezialisten am Firmensitz in Münster (Westf.), Deutschland sorgen für den sicheren 24/7 Betrieb und werden dabei unterstützt von den kompetenten Fachkräften der Tochterunternehmen woyn auf den Philippinen und der nicos Australia.
Um ihren Kunden den bestmöglichen Schutz vor Bedrohungen aus dem Internet und vor Cyberattacken zu bieten, werden die Leistungen des nicos Service Operation Center ergänzt durch das Cyber Defense Center mit den Spezialisten des Tochterunternehmens nicos cyber defense.
Neue Möglichkeiten intelligenter Kommunikationswege zu erforschen und zu entwickeln, steht im Fokus der nicos Research & Development Spezialisten.