itsecurity
JULI/AUGUST 2018

DAS SPEZIAL

ACCESS GOVERNANCE

TRANSPARENZ AUF KNOPFDRUCK

Thomas Gertler und Jürgen Bähr,
Geschäftsführer G+H Systems GmbH

UNIFIED ENDPOINTS

Cyber-Attacken
in Echtzeit stoppen

DATEILOSE ANGRIFFE

AV-Lösungen
sind machtlos

MANAGED SECURITY SERVICES

Mehr als eine
günstige Alternative

ab Seite 8

www.it-daily.net

noris network

#DIGITALISIERUNG get IT ready

IT-TRANSFORMATION | IT-STRATEGIE | AGILE

PRIVATE | PUBLIC CLOUD | OPEN STACK

GOVERNANCE & COMPLIANCE
EU-DSGVO | RISIKOMANAGEMENT
INFORMATIONSSICHERHEIT | IT-SECURITY
SIEM | SECURITY-MONITORING

INFORMATION UND ANMELDUNG MIT DEM CODE: secure-it

www.digitalisierung-get-it-ready.de

Mit von der Partie

Hewlett Packard Enterprise

DELL EMC · FORTINET · NetApp Data Driven · SentinelOne · TechData Advanced Solutions · vmware

22

4

COVERSTORY

INHALT

TRANSPARENZ AUF

ACCESS GOVERNANCE – DATENSCHUTZ UND BERECHTIGUNGEN.

it security: *Herr Gertler, Sie und Herr Bähr blicken zusammen auf mehr als 30 Jahre Erfahrung im Bereich Identity & Access Management zurück. Sie haben mit daccord vor 8 Jahren eine eigene Access Governance-Software auf den Markt gebracht. Was war der Auslöser für diese Entwicklung?*

Thomas Gertler: Wir haben in unseren Kundengesprächen immer wieder festgestellt, dass es vielen IT-Verantwortlichen nicht möglich war, schnell und einfach einen Überblick über die Zugriffsberechtigungen im Unternehmen zu erhalten. Bis dahin war es ein kosten- und zeitintensiver Vorgang manuell – oftmals in Excelsheets – alle Informationen zu erfassen. Zudem schlichen sich auch häufig Fehler ein. Gerade in Hinblick auf gesetzliche Vorgaben, wie ganz aktuell die DSGVO, gewinnen automatisierte Lösungen, die auf Knopfdruck alle notwendigen Informationen zur Verfügung stellen und kontinuierlich bereithalten, immer mehr an Bedeutung. Damit wir diese Transparenz auch möglichst lückenlos über alle Systeme in der IT-Landschaft im Unternehmen gewährleisten können, war es uns von Anfang an besonders wichtig, herstellerunabhängig zu sein.

it security: *Die DSGVO war in den vergangenen Wochen allgegenwärtig. Haben Sie den Eindruck, dass die Unternehmen fit sind in Sachen Datenschutz?*

Jürgen Bähr: In unserem Geschäftsalltag erleben wir durchaus, dass viele Unternehmen sich der Gefahren durch Datenmissbrauch und Datenabfluss sowie deren Folgen bewusst sind. Vertrauliche Unternehmensinformationen, Kundendaten und Zugriffsberechtigungen werden aber dennoch oftmals nicht ausreichend geschützt. Das geschieht aus meiner Sicht nicht aus Unkenntnis, sondern liegt gerade im Mittelstand daran, dass zu wenig Zeit und Ressourcen für das Thema Sicherheit zur Verfügung stehen. Das kann für einen IT-Verantwortlichen im Arbeitsalltag zu einer unmöglichen Mission werden. Hier sind einfache und schnelle Lösungen ein echter Mehrwert. Denn spätestens seit dem Stichtag der DSGVO müssen Unternehmen für den Schutz aller personenbezogenen Daten sorgen. Die Konsequenzen bei Nichteinhaltung der gesetzlichen Vorgaben sind abgesehen vom Imageschaden auch finanziell schmerzhaft.

> OFTMALS FEHLT ES IN DER KOMPLEXEN IT-LANDSCHAFT BEI DER MITARBEITERERFASSUNG AN EINER ÜBERSICHTLICHEN DARSTELLUNG DER RECHTESTRUKTUREN.
>
> Thomas Gertler, Geschäftsführer G+H Systems GmbH www.guh-systems.de

it security: *Die Datenschutzgrundverordnung stellt viele Unternehmen vor eine große Herausforderung. Wie nehmen Sie die Herangehensweise der IT-Verantwortlichen in Bezug auf die DSGVO wahr?*

Jürgen Bähr: Wir stellen immer wieder fest, dass in vielen Unternehmen die Unsicherheit überwiegt. Anstehende Prüfungen und die möglichen hohen Strafen, die bei Verstößen drohen, erhöhen zusätzlich den Druck auf die Unternehmen. Sie erleben die DSGVO tendenziell eher als Belastung und haben das Gefühl, dass ihnen die Zeit wegrennt. Umso wichtiger ist es für uns, Unternehmen in dieser Phase sinnvolle, einfache Lösungen an die Hand zu geben. Tools, die schnell einsatzbereit sind und sofort Entlastung bieten sowie Unsicherheiten beseitigen.

it security: *Wo sehen Sie die größten Schwierigkeiten für Unternehmen in Hinblick auf die Mitarbeiterberechtigungen?*

Thomas Gertler: Oftmals fehlt es in der komplexen IT-Landschaft bei der Mitarbeitererfassung an einer übersichtlichen Darstellung der Rechtestrukturen. Ein Mitarbeiter wechselt die Abteilung, ein neuer kommt – die Zuständigkeiten im Unternehmen können sich schnell ändern. Neue Zuständigkeiten beinhalten in der Regel auch neue Berechtigungen und dabei ist fast noch wichtiger, alte Berechtigungen wieder zu entziehen. Zusätzlich erschwert die gewachsene Struktur aus verschiedenen Systemen und Anwendungen die Kontrolle dieser Zugriffsrechte. Für IT-Verantwortliche und Fachabteilungen ist es eine Herausforderung, hier den Überblick zu bewahren. Die Rechtestrukturen transparent zu halten, kann viel Zeit in Anspruch nehmen und kostenintensiv sein. Immer wieder kommt es zu fehlerhaften Berechtigungen, die in der

KNOPFDRUCK

> FÜR UNS IST ES WICHTIG UNTERNEHMEN SINNVOLLE, EINFACHE LÖSUNGEN AN DIE HAND ZU GEBEN. TOOLS, DIE SCHNELL EINSATZBEREIT SIND UND SOFORT ENTLASTUNG BIETEN.
>
> Jürgen Bähr,
> Geschäftsführer
> G+H Systems GmbH
> www.guh-systems.de

komplexen IT-Landschaft schnell übersehen werden. Das kann die IT-Sicherheit eines Unternehmens erheblich gefährden.

? **it security**: *Wie können Unternehmen die Kontrolle der Zugriffsrechte im Sinne der DSGVO reibungslos umsetzen?*

Thomas Gertler: Es gibt Software-Tools, die bei der Umsetzung der Datenschutzgrundverordnung unterstützen und den Prozess dadurch wesentlich vereinfachen. Das Gleiche kann eine Access Governance-Software wie daccord für die Verwaltung der internen Rechtestrukturen leisten. Für ein effektives Management der Zugriffsrechte erfüllt eine DSGVO-konforme Access Governance-Lösung sämtliche Anforderungen. Die Software schafft Transparenz über die Rechtestrukturen im Unternehmen und verringert so den Verwaltungsaufwand in der IT-Abteilung.

Jürgen Bähr: Die Verantwortlichen sollten darauf achten, dass die Access Governance-Software sämtliche Zugriffsrechte der eingesetzten Cloud- und On-Premise-Anwendungen einliest und diese übersichtlich in personalisierten Web-Frontends darstellt. So lassen sich alle relevanten Informationen zu den Mitarbeiterberechtigungen auf einen Blick einsehen und überprüfen. Das spart neben Zeit auch Kosten. Die interne IT-Abteilung wird deutlich entlastet und kann die Verantwortung über die Kontrolle von Zugriffsrechten erstmalig an Fachabteilungen übergeben. Mit einer zusätzlichen Alarmierungsfunktion bei Abweichungen in der Berechtigungsvergabe ist man auf der sicheren Seite. Denn so ist eine unmittelbare Reaktion möglich, um eventuelle Unstimmigkeiten schnell zu beheben und Risiken zu minimieren.

? **it security:** *Wie sehen Sie Access Governance-Lösungen im Vergleich zu IAM-Systemen?*

Thomas Gertler: Auch wenn beim Kunden bereits ein IAM-System besteht, ist eine Access Governance-Software wie daccord sinnvoll, um zu kontrollieren, welche Daten tatsächlich im Zielsystem ankommen. Aufgrund unserer langjährigen Erfahrung im IAM-Bereich unterstützen wir viele Unternehmen bei der Implementierung ihres IAM-Systems. Hier stellen wir immer wieder fest, wie wichtig und hilfreich es ist, eine Access Governance-Software zusätzlich im Einsatz zu haben. Ein IAM-System ist sinnvoll, aber zum Einstieg nicht zwingend notwendig: Mit daccord kann der Anwender zum Beispiel individuelle Rollenmodelle anlegen. So lassen sich Soll-Berechtigungen für bestimmte Abteilungen oder Positionen klar definieren. Auf Knopfdruck zeigt die Software Vergleiche zwischen dem Soll- und dem Ist-Zustand. Über- oder Unterberechtigungen der Mitarbeiter werden so schnell aufgedeckt, und Löschungen können über die Anwendung direkt initiiert werden. Bestenfalls erfolgt die Kommunikation mit einem IAM-System, das den Workflow automatisiert. In einem ersten Schritt kann es aber auch einfach eine Mail an den Verantwortlichen oder Ähnliches sein. Da sind wir mit daccord ganz flexibel – je nachdem, wie die IT im Unternehmen organisiert ist.

? **it security:** *Wer gehört zur Zielgruppe Ihrer Access Governance-Lösung? Großunternehmen oder auch der Mittelstand?*

Jürgen Bähr: Da sprechen Sie einen wichtigen Punkt an. daccord ist derzeit sowohl bei Großunternehmen als auch im Mittelstand erfolgreich im Einsatz. Ob Banken, Krankenhäuser, Behörden oder kleine und mittelständische Betriebe – eine Access Governance-Software eignet sich für Unternehmen jeder Größe. Denn entscheidend ist nicht die Unternehmensgröße, sondern die Wichtigkeit der zu kontrollierenden Daten. Aufgrund des transparenten Lizenzmodells sowie einer kostengünstigen, individuell ausgearbeiteten Schnellanalyse im Vorfeld, ist unsere Lösung für jedes Unternehmen interessant, das bei der Kontrolle von Zugriffsberechtigungen Zeit- und Kostenersparnisse sucht sowie den gesetzlichen Anforderungen effektiv begegnen möchte.

! **it security:** *Herr Gertler, Herr Bähr, wir danken für das Gespräch.*

DSGVO UND FACHKRÄFTEMANGEL

GEMANAGTE SECURITY SERVICES ENTLASTEN DIE UNTERNEHMENS-IT.

DIE UMSETZUNG DER DSGVO BEDEUTET FÜR UNTERNEHMEN UND ORGANISATIONEN VOR ALLEM MEHR DOKUMENTATION.

Dariush Ansari, Geschäftsleiter Network Box Deutschland GmbH | www.network-box.eu

Das alte Bundesdatenschutzgesetz wurde durch die neue Europäische Datenschutz-Grundverordnung (DSGVO) abgelöst. Immer noch herrscht Unsicherheit in vielen IT-Abteilungen, wie personenbezogene Daten nach dem Stand der Technik zu schützen sind. Hinzu kommt der Fachkräftemangel, der für viele Unternehmen kritischer ist als die DSGVO. Erfahrene Managed Security Service Provider (MSSP) können als Partner die Absicherung der IT-Infrastruktur sowie die Umsetzung der technischen Datenschutzregeln unterstützen.

Die IT ist ein Bereich, der mit ständigen Änderungen und neuen Anforderungen konfrontiert wird. Die DSGVO ist zwar umfangreich, aber eben nur eine dieser Änderungen und hat zudem nicht nur etwas mit IT zu tun. Mit diesen ständig wachsenden Anforderungen Schritt zu halten, bedeutet jedoch viel Arbeit, und längst nicht jedes Unternehmen ist in der Lage, eine eigene IT-Sicherheitsabteilung zu unterhalten und mit dem notwendigen Personal zu besetzen. Vor allem kleine und mittlere Unternehmen (KMU) sind vom Fachkräftemangel in der IT betroffen.

Doch genau diesen Fachkräftemangel kann ein MSSP direkt abdecken. Ein externes Security-Team ist für IT-Abteilungen eine starke Entlastung und bietet auch wirtschaftliche Vorteile: Kommt es zum Beispiel zu einem Defekt der Hardware, ist ein Austausch in kurzer Zeit in den meisten Service-Verträgen enthalten. Wächst das Unternehmen, kann der Service – beispielsweise in Mietmodellen – oftmals unkompliziert skaliert werden. Die hohen Personalkosten für entsprechend geschulte IT-Experten entfallen fast vollständig, ebenso wie hohe Investitionskosten für Hardware. Je nach Situation gibt es auch passende Mietmodelle. Die sind flexibel anpassbar und bieten einen kalkulierbaren Kostenrahmen.

DSGVO und MSSP

Die Umsetzung der DSGVO bedeutet für Unternehmen und Organisationen vor allem mehr Dokumentation. Sie müssen jederzeit darüber Auskunft geben können, welche Daten sie zu welchem Zweck erheben. Kommt es zu einem Datenschutzvorfall, ist es hilfreich, für eine schnelle Meldung auf die benötigten Informationen zurückgreifen zu können. Ein MSSP, der unerlaubte Aktivitäten im Netzwerk dokumentiert, kann einige dieser Informationen liefern und die Administratoren mit transparenten Reports unterstützen. Während eines sicherheitsrelevanten Vorfalles erleichtert die Kooperation mit einem MSSP zusätzlich Gegenmaßnahmen und verhindert unnötigen Schaden.

Fazit

Vor allem KMU haben unter dem aktuellen Fachkräftemangel in der IT zu leiden, und die DSGVO bedeutet für viele Unternehmen eine zusätzliche Belastung. Ein erfahrener MSSP kann für Administratoren in Unternehmen eine signifikante Entlastung sein. Bei der Auswahl eines passenden Anbieters sollten wirtschaftliche Aspekte ebenso berücksichtigt werden wie technische. Flexibel skalierbare Mietmodelle mit kurzen Kündigungsfristen gehen besonders auf die Bedürfnisse kleiner und mittlerer Betriebe ein. Mit transparenten Reports, vor allem über unerlaubte Aktivitäten im Netzwerk, sowie Warnungen und guter Unterstützung bei einem Sicherheitsvorfall im Netzwerk sind fristgerechte Meldungen nach den DSGVO-Regeln an die Datenschutzbehörden kein Problem. Letztendlich werden Unternehmen, die nachweislich über einen gut funktionierenden Datenschutz verfügen, diesen sogar als Wettbewerbsvorteil erleben können.

Dariush Ansari

Die Wikinger sind hier, um uns zu beschützen

Clavister ist ein schwedisches Cybersicherheitsunternehmen mit der festen Überzeugung, dass robuste Netzwerksicherheit jedermanns Sache ist. Mit einem virtuellen und physischen Ökosystem schützen wir Geschäftsprozesse und stellen sicher, dass unsere Kunden die bestmögliche Sicherheit vor der wachsenden Bedrohungslandschaft haben. Wir haben heute zwar Schwert und Axt gegen Code eingetauscht, aber wir haben nach wie vor unseren Wikingergeist, der besagt, dass die beste Cyber-Verteidigung ein starkes Sicherheitssystem ist.

Erfahren Sie mehr unter clavister.com/Die-Wikinger

clavister
CONNECT . PROTECT

SECURITY BY SWEDEN

SICHERHEIT AUS

UNTERNEHMEN DENKEN NOCH NICHT WEIT GENUG.

it security sprach mit Thomas Gross, Sales Director Dach bei Clavister, über aktuelle Gefahren und den Vorteil, ein europäisches Unternehmen zu sein.

it security: *Herr Gross, Cybersecurity ist ein großes Problem in der heutigen Welt. Wie sehen Sie diese im größtmöglichen Blickwinkel? Halten Sie einen „Cyberwar" für eine reale Bedrohung? Und ist besonders kritische Infrastruktur in Gefahr?*

Thomas Gross: Ich denke, gerade die letzten Jahre haben uns gezeigt, dass die Bedrohung absolut real ist. Häufig ist dies nicht einmal der Komplexität der Angriffe geschuldet, sondern eher der mangelhaften Verteidigung. Man kann nicht erwarten, dass eine unzureichende Lösung optimalen Schutz gewährt.

Und natürlich ist auch ein „Cyberwar" eine nicht zu unterschätzende Gefahr, da es für viele Gruppierungen eine einfache und schwer zurückzuverfolgende Möglichkeit ist, die eigenen Interessen durchzusetzen. Kritische Infrastruktur spielt da auch eine besondere Rolle, denn wo es für Unternehmen sicherlich ärgerlich oder vielleicht gar existenzbedrohend sein kann, wenn ein Vorfall passiert, hängen bei einigen Bereichen der kritischen Infrastruktur Menschenleben davon ab.

it security: *Was bereitet Ihnen als Anbieter von Security-Lösungen Sorgen? Was sind die größten Bedrohungen für Ihre Geschäftskunden?*

Thomas Gross: Die größten Bedrohungen der nahen Zukunft werden weiterhin Verschlüsselungstrojaner sein, die definitiv das Potential haben, die Geschäftswelt noch eine ganze Weile in Atem zu halten. Was uns am meisten Sorge bereitet ist die Tatsache, wie einfach man heutzutage an entsprechende Bausätze für Schadsoftware herankommt, es kann faktisch jeder einfach seinen eigenen, individuellen Trojaner zusammenklicken und auf die Welt loslassen.

it security: *Denken Sie, dass Unternehmen die Bedrohung ernst genug nehmen? Falls nein, was ist der Grund dafür?*

Thomas Gross: Leider denken auch heute noch viele Unternehmen nicht weit genug. Es wird an allem gespart und gehofft, dass es einen schon nicht treffen wird. Ganzheitliche Sicherheitskonzepte, die von einer vernünftigen Firewall, über einen starken Endpoint-Security-Client bis hin zu Multifaktor-Authentifizierung reichen, gibt es leider noch immer viel zu selten. Dabei gibt es auch Lösungen wie unsere, die für den KMU-Bereich problemlos einzusetzen und zudem preislich extrem attraktiv sind. Hier muss in den Unternehmen einfach ein Umdenken stattfinden.

it security: *Clavister kommt aus Schweden, operiert allerdings global. Hat es für Ihre Lösungen irgendwelche Vorteile, aus Schweden zu kommen?*

Thomas Gross: Ganz eindeutig! Neben der Tatsache, dass wir als europäischer Anbieter natürlich sowohl den Fokus auf dem europäischen Markt haben und entsprechend unsere Strategie und Produktentwicklung darauf ausrichten, ist es auch eine Vertrauensfrage.

Wir sichern zum Beispiel bereits seit 2009, also lange vor den Enthüllungen von Edward Snowden, unseren Kunden Backdoorfreiheit zu, die wir durch unser eigenes Betriebssystem auch sicherstellen können. Mittlerweile werden sogar unsere Hardware-Appliances in Schweden gefertigt, um auch dort die Möglichkeiten der Manipulation maximal einzuschränken. Andere Anbieter unterliegen staatlichen Regularien, die es in Schweden nicht gibt.

it security: *Das ist interessant. Erläutern Sie uns, was „no back doors" eigentlich bedeutet?*

Thomas Gross: Für uns bedeutet das, dass wir als Hersteller weder selber Zugriff auf die Firewalls haben, noch Zugang für Dritte gewähren wollen oder können, wie es etwa im PatriotAct der Vereinigten Staaten von dortigen Anbietern verlangt wird. In unseren Augen ist dies auch ein klarer Fall, dass derartiges nichts in einer Security-Lösung zu suchen hat, denn es besteht immer die Gefahr, dass solche Backdoors auch von anderen Parteien ausgenutzt werden.

it security: *Sie sagen also, dass amerikanische oder auch chinesische Firmen kompromittiert sind durch den Einbau von Hintertüren, die Zugriff auf die root und kernel Verzeichnisse bieten. Wie können wir Clavister vertrauen?*

Thomas Gross: Wir entwickeln unseren Code selbst und nutzen nicht, wie oft auf dem Markt anzutreffen, einfach fertige OpenSource-Komponenten. Weiterhin geben wir die bereits erwähnte schriftliche Garantie. Wem das immer noch nicht reicht, der kann gerne in unserem Headquarter in Örnsköldsvik vorbeikommen und ein Code-Review machen.

it security: *Erzählen Sie uns etwas über die 20 Jahre, die Clavister bereits am Markt ist.*

Thomas Gross: Letztlich ist es eine ganz klassische „Von der Garage zum internationalen Unternehmen"-Geschichte, wie man sie ja gerade in der IT öfters findet, mit einem kleinen, aber besonderen Unterschied:

Es ist unsere Leidenschaft für IT-Security und nicht das Bestreben, das Unternehmen möglichst groß zu machen und dann gewinnbringend zu verkaufen, was uns alle hier immer weiter antreibt. Wer bei Clavister arbeitet, wird in eine große Familie aufgenommen, in der mittlerweile über 30 unterschiedliche Nationalitäten gemeinsam an der Weiterentwicklung einer extrem spannenden Technologie arbeiten. Und bis auf wenige Ausnahmen bleiben die Menschen dann auch bei Clavister,

LEIDENSCHAFT

> ES IST UNSERE LEIDENSCHAFT FÜR IT-SECURITY UND NICHT DAS BESTREBEN, DAS UNTERNEHMEN MÖGLICHST GROSS ZU MACHEN UND DANN GEWINNBRINGEND ZU VERKAUFEN, WAS UNS ALLE HIER IMMER WEITER ANTREIBT.
>
> Thomas Gross, Sales Director Dach, Clavister, www.clavister.com

was in meinen Augen ganz klar für das Unternehmen spricht.

? **it security:** *Das ist eine unglaubliche Geschichte. Und wenn ich richtig verstanden habe, sind auch viele der Gründer noch immer im Unternehmen?*

Thomas Gross: Ja, unser CEO John Vestberg ist ein gutes Beispiel dafür, aber auch viele andere Kollegen und Managementteam-Mitglieder sind von Anfang an dabei. Ich habe im Laufe der Jahre auch mehrmals mitbekommen, wie Kollegen gewechselt und nach einiger Zeit wieder zu Clavister zurückgekommen sind.

? **it security:** *Ihr deutsches Team ist relativ neu, Sie sind allerdings schon seit einigen Jahren im Unternehmen. Erzählen Sie uns davon.*

Thomas Gross: Ich bin seit mittlerweile 13 Jahren bei Clavister und habe den Channel bis auf die letzten zwei Jahre nahezu alleine aufgebaut und betreut. Natürlich erreicht man so irgendwann einen Punkt, wo dann kein wirkliches Wachstum mehr möglich ist und die Qualität der eigenen Arbeit zu leiden beginnt und auch den eigenen Ansprüchen nicht mehr genügt. Umso mehr freue ich mich nun darauf, mit dem neuen Team durchstarten zu können. Wir haben uns entschlossen, das Team dezentral aufzustellen, um eine bessere und intensivere Partnerbetreuung zu ermöglichen, als dies von einem einzelnen Büro aus möglich wäre.

Ein bisschen wehmütig bin ich natürlich schon, da mit meiner neuen Tätigkeit sich verständlicherweise auch mein eigener Schwerpunkt verschiebt, auf der anderen Seite bieten sich für uns als Unternehmen nun ganz neue Möglichkeiten. Und ich habe ein großartiges Team an meiner Seite, welches in der nahen Zukunft auch noch weiterwachsen soll.

? **it security:** *Wer sind Ihre Lieblingskunden und warum?*

Thomas Gross: Das lässt sich so pauschal gar nicht sagen, wir haben Kunden aus allen Branchen und in allen Größen, da die Lösungen von Clavister darauf ausgelegt sind, möglichst flexibel zu sein und eine breite Palette an Funktionen bieten. Am spannendsten und befriedigendsten sind sicherlich die Projekte, wo ein Kunde vor einer konkreten Problematik steht, die durch seine bisherige Lösung nicht abgedeckt werden kann und wir ihm mit der Clavister weiterhelfen können.

! **it security:** *Herr Gross, wir danken Ihnen für dieses Gespräch.*