iX extra Oktober 2020

iX Security

Eine Sonderveröffentlichung der Heise Medien GmbH & Co. KG

IT-Sicherheitstrends und -produkte

Security Operations Center intern oder als Managed Service

Beste Reaktion

Seite 118

Videokonferenz-Dienstleister im Datenschutztest

Unvorbereitet

Seite 122

Sicherheit für Container

Teure Agilität

Seite 126

iX extra zum Nachschlagen:
www.ix.de/extra

Beste Reaktion

Security Operations Center intern oder als Managed Service

Die Funktionen eines Security Operation Center sind für die Abwehr von Angriffen auf die Unternehmens-IT unverzichtbar. Doch was tun, wenn im eigenen Unternehmen nicht genug Know-how steckt? Dienstleister können hier unterstützen – auch teilweise.

Bekanntlich stellt sich heutzutage nicht mehr die Frage, ob, sondern nur noch, wann ein Unternehmen Opfer eines Angriffs wird. Daher sind umfassende Vorkehrungen für die Cybersicherheit, auch in Form eines SOC (Security Operations Center), ein Muss, um Angriffe überhaupt erkennen und dann schnell und angemessen reagieren zu können. Die Frage ist, ob das SOC intern betrieben, an einen Dienstleister ausgelagert oder hybrid gemanagt wird.

SOC als eigene Sicherheitsleitstelle

Das SOC stellt eine eigene Organisationseinheit im Unternehmen dar, die meistens außerhalb der IT- oder OT-Abteilungen (Operational Technology) angesiedelt ist. Wichtig ist bei der organisatorischen Zuordnung, die Nähe zur Technik zu wahren und gleichzeitig dem Prinzip der Aufgabentrennung zu folgen. Daher sollte das SOC dem CISO (Chief Information Security Officer) untergeordnet sein. Als Sicherheitsleitstelle werden im SOC alle digitalen Netzwerke, Server, digitalen Geräte und Informationen und auch der Datenfluss überwacht.

Monitoring, Erkennung und Reaktion (durch ein Computer Emergency Response Team, CERT, oder ein Computer Security Incident Response Team, CSIRT) liegen so vereint unter einem Dach. Weil IT und OT immer stärker zusammenwachsen, sollte dies für beide Welten stattfinden. Bei Auffälligkeiten leitet das SOC Gegenmaßnahmen ein, die die Betriebsteams umsetzen. Das SOC berichtet über seine Aktivitäten an den CISO beziehungsweise das Topmanagement.

Häufig sind SOCs als Kommandostand aufgebaut, an dem Mitarbeiter auf Monitoren die IT- und OT-Systeme überwachen. Sie agieren einerseits proaktiv und suchen mögliche Schwachstellen in den Systemen oder Bedrohungen aus der Außenwelt. Andererseits reagieren sie auf Angriffe und Eindringversuche. Hierfür ist es wichtig, ein sogenanntes „Security Playbook“ zu erstellen, damit es möglich ist, standardisiert und teamübergreifend auf Vorfälle zu reagieren. Die eingesetzten Schutzmaßnahmen sind sowohl technischer Natur, beispielsweise Optimierung von Firewalls, Aufsetzen eines IPS/IDS oder einer Proxy-Infrastruktur, von Identity and Access Management oder die Härtung von Systemen, als auch organisatorischer Art, wie etwa die Anpassung von Nutzerrechten oder Prozessen.

Frühe Erkennung eines Angriffs

Infolge des permanenten Monitorings der Datenflüsse, der Schwachstellen und des Sicherheitsniveaus lassen sich Angriffe frühzeitig erkennen und oft bereits im Vorfeld verhindern. Die Verantwortlichkeiten müssen klar geregelt sein und Maßnahmen schnell und umfassend auf den Weg gebracht werden. Im Krisenfall arbeitet das SOC eng mit dem Krisenstab zusammen.

Mitarbeiter im SOC sind als Spezialisten bestens mit den Eigenheiten der Unternehmens-IT und -OT vertraut, sind aber wegen des Fachkräftemangels oft schwer zu finden. Auch bedeutet das Einrichten eines eigenen SOC viel Aufwand und „Tuning“ der Systeme sowie die Erstellung von Regeln, die Alarme auslösen, auch Use Cases genannt. Struk-

Die vielfältigen Aufgaben eines SOC kann sich ein Unternehmen auch mit dem Dienstleister teilen – nur sinnvoll muss es sein.

turen und Prozesse müssen grundlegend aufgesetzt und Überwachungssysteme angeschafft werden. Der zunehmende Bedarf an KI und Automatisierung zur Erkennung und Behandlung von Sicherheitsvorfällen stellt Unternehmen vor weitere Herausforderungen bei der Rekrutierung geeigneter Mitarbeitender.

SOC als Managed Service – Hilfe von außen

Der Betrieb eines SOC kann auch als Managed Service an einen Dienstleister ausgelagert werden. Externe Anbieter übernehmen dann die Überwachung der Datenflüsse und die Kontrolle des Schutzniveaus. Je nach Vereinbarung kann der Dienstleister auch Anpassungen an den IT- und OT-Systemen vornehmen, wobei hier die Aufgabentrennung äußerst wichtig ist. Zugriffe müssen genau geregelt sein und auf einem Vertrauensverhältnis beruhen.

Das Level des Sourcing kann auch so zugeschnitten sein, dass das Monitoring zwar an einen Dienstleister gegeben, die Behandlung von Sicherheitsvorfällen aber intern durchgeführt wird. So kann der Dienstleister den vollen Leistungsumfang eines SOC erbringen, und gleichzeitig bleibt die „Intelligenz", also das Wissen, im Unternehmen. Bei diesem sogenannten hybriden Ansatz werden feste Incident-Response-Prozesse etabliert, die klar regeln, wie mit Vorfällen umzugehen ist, und die eine Brücke zwischen externem Dienstleister und interner Organisation schlagen.

SOC as Managed Service (SOCaMS) ist besonders für kleinere Unternehmen mit weniger Ressourcen eine gute Alternative, bietet aber auch grundsätzliche Vorteile, da ein Lernen aus der Erfahrung von anderen Unternehmen möglich ist. Nach Bedrohungen, die bei einem Kunden bekannt werden, kann der Dienstleister auch bei anderen Kunden suchen oder Use Cases einfach übernehmen. Beide Ansätze haben Vor- und Nachteile, deshalb wählen die meisten Unternehmen hybride Ansätze.

SOC versus SOCaMS

Für ein SOC im Unternehmen spricht die Tatsache, dass die Mitarbeiter im Idealfall mit der eigenen IT und OT bestmöglich vertraut sind. Das Management hat so für alle Cybersicherheitsfragen klare Ansprechpartner direkt vor Ort. Durch die Dokumentation aller digitalen Vorgänge im SOC können Synergien zu Compliance- und Datenschutzthemen geschaffen werden. Eigene SOCs haben allerdings begrenztere Ressourcen und oft nur das eigene Unternehmen im Blick. Auch ist es, bedingt durch den Fachkräftemangel, schwierig, Mitarbeiter im Unternehmen zu halten.

Externe Dienstleister, die mehrere Kunden absichern, haben hingegen einen besseren 360-Grad-Blick auf aktuelle Bedrohungen und können Probleme von Kunde A auf Kunde B übertragen. Beim SOCaMS können mehr mögliche Bedrohungen und Schwachstellen identifiziert werden, da diese bereits bei anderen Kunden gefunden wurden. Die Aufbauphase erfolgt deutlich schneller, weil Systeme und Erfahrungen bereits vorhanden sind.

Auch können bei SOCaMS weniger kompliziert kurzfristig benötigte zusätzliche Services oder Ressourcen dazugebucht werden. Zudem sind Mitarbeiter eines externen Dienstleisters im Notfall häufig in der Lage, geübter zu reagieren, weil sie durch weitere Kunden mehr Erfahrung mit Notfällen haben.

Des Weiteren kann der nötige 24/7-Dienst bei einem externen Dienstleister, der extra dafür bezahlt wird, oft konstanter realisiert werden. Und schließlich liefert der Dienstleister die Management-Reports meist mit.

Ein SOCaMS hat aber auch Nachteile: Mitarbeiter, die ihre Zeit nur dem eigenen Unternehmen widmen, kennen die eigenen Systeme besser. Auch fällt die Kommunikation, besonders zum Management, durch ein internes Vertrauensverhältnis leichter. In der Praxis empfiehlt sich daher oft eine Kombination beider Ansätze, der hybride Ansatz.

Hybrider Ansatz – Vorteile beider Welten

Für die nötige 24/7-Überwachung im SOC sind mindestens acht Mitarbeiter notwendig. Die Aufgaben im SOC sind verteilt, wobei die grundlegende Überwachung der Datenflüsse meist durch ein automatisiertes Security Information and Event Management (SIEM) durchgeführt wird. Tier-1-Analysten überwachen und bearbeiten, sofern das zügig möglich ist, die Warnmeldungen des SIEM. Tier-2-Analysten bearbeiten und bewerten die SIEM-Meldungen dann, wenn diese mehr Aufwand erfordern.

Zudem gibt es sogenannte Threat Hunter, die gezielt nach Schwachstellen und Bedrohungen suchen, und Konfiguratoren, die basierend auf der Arbeit der Analysten und Threat Hunter Anpassungen an den IT- und OT-Systemen vornehmen lassen. Dazu koordiniert zumeist ein SOC-Manager die Arbeit und vertritt sie gegenüber dem Management oder dem Kunden. Wichtig ist, dass die einzelnen Aufgaben von unterschiedlichen Personen ausgeführt werden. Ein Konfigurator sollte nicht die Sicherheit seiner eigenen Anpassungen testen und die Schwachstellensuche sollte außerhalb des Analyserahmens laufen.

Bei der Kombination beider Ansätze bietet es sich an, die Aufteilung der Aufgaben grob anhand der Trennlinien der Mitarbeitergruppen vorzunehmen. Eigene Analysten können durch externe Threat Hunter oder Threat Reports unterstützt werden, um so den Vorteil einer unvoreingenommenen Außensicht zu nutzen. Das externe SOC spielt dabei seine Expertise beim Erkennen und das interne SOC beim Abarbeiten aus. Die Anpassungen eines internen Konfigurators lassen sich gut durch externe Analysten überwachen.

In der Praxis werden häufig Routinearbeiten wie das Auswerten von Logdateien und die Ereignisprüfung (Tier 1) ausgelagert. Tier 2 erfolgt dann durch interne und externe Kräfte gemeinsam, da hierfür viel internes Wissen nötig ist. Die Umsetzung der Maßnahmen wiederum verbleibt dann komplett intern. Die Schnittstelle zwischen extern und intern liegt daher oft bei Tier 2 und die Trennung erfolgt zwischen Analysten und dem Incident Response Handling.

Um die beste Kombination der Aufgabenteilung zu finden, muss das Unternehmen die eigene Situation richtig bewerten. Welche Ressourcen und welches Know-how sind im Unternehmen selbst vorhanden? Wo ist externe Hilfe erforderlich? Das Zusammenspiel von externen und internen Kräften sollte klar geregelt sein. Kontaktnummern müssen immer zur Hand und das Vorgehen im Ernstfall durch Notfallpläne eindeutig geklärt sein.

Einige Dienstleister aus dem Bereich Incident Response

Unternehmen	Link
Avantec	https://www.avantec.ch/services/incident-response/
Airbus Cyber Security	https://airbus-cyber-security.com/de/produkte-und-services/respond/
Broadcom	https://www.broadcom.com/products/cyber-security/network/atp/network-forensics-security-analytics
Check Point	https://www.checkpoint.com/support-services/threatcloud-incident-response/
Cyber Triage	https://www.cybertriage.com/
DfN-CERT	https://www.dfn-cert.de/leistungen/incidentresponse.html
D3 Security	https://d3security.com/
Fast Detect	https://www.fast-detect.de/it-forensik/leistungen/incident-response/
Gdata	https://www.gdata.de/business/security-services/incident-response
Deloitte	https://www2.deloitte.com/de/de/pages/risk/solutions/cyber-incident-response.html
FireEye	https://www.fireeye.de/mandiant/incident-response.html
Forcepoint	https://www.forcepoint.com/cyber-edu/incident-response
Helmich	https://www.helmich.de/welt-der-it-security/irt-incident-response-team
IBM Resilient	https://www.ibm.com/de-de/marketplace/resilient-soar-platform
Nviso	https://www.nviso.eu/de/service/8/24-stunden-incident-response
One Consult	https://www.oneconsult.com/de/cyber-security-incident-response/
R-tec	https://www.r-tec.net/incident-response-service.html
Schutzwerk	https://www.schutzwerk.com/de/40/Incident-Response-Management.html
Secudor	https://secudor.de/incident-response/
Splunk	https://www.splunk.com/de_de/cyber-security/incident-response.html
SYSS	https://www.syss.de/leistungen/schulung/secu2-incident-response/
touringpoint	https://turingpoint.de/consulting/incident-response-management/
8 Com Cyber Security	https://www.8com.de/incident-response

Best Practices

Oberste Priorität beim Betrieb eines SOC in der Praxis muss sein, dass die Einheit tatsächlich Zugriff auf alle Daten im Unternehmen hat. Laut einer Studie des Ponemon Institute gibt die deutliche Mehrheit von über 500 befragten IT-Sicherheitsverantwortlichen an, dass dieser Zugriff nicht ausreichend umgesetzt ist. Auch müssen SOCs gut in den Rest des Unternehmens eingebunden sein. Der Nutzen des SOC für das Unternehmen muss deutlich sein und entsprechende Unterstützung vom Management kommen.

Die Nähe zur Technik ist wichtig, um keinen Elfenbeinturm zu bauen. Nur wenn ausreichend Transparenz und die Bereitschaft zur Verantwortungsübertragung auf das SOC vorhanden sind, kann ein effizientes Funktionieren des SOC gewährleistet sein. Zudem ist es wichtig, im SOC interoperable Technik einzusetzen. Bei der Aufteilung des SOC-Betriebs auf intern und extern müssen alle Anwendungen gut ineinandergreifen.

Ein weiteres Praxisproblem besteht im Finden und Halten der SOC-Mitarbeiter. SOC-Spezialisten sind sehr begehrt, gleichzeitig sind sie einem hohen Stresslevel ausgesetzt. Vorhandene Mitarbeiter müssen daher gut unterstützt werden und ein Plan für Backups sollte vorhanden sein. Letztlich wird die Arbeit eines SOC durch den regelmäßigen Austausch mit anderen SOCs deutlich erleichtert. Über Organisationsgrenzen hinweg können Schwachstellen und Bedrohungen besser erkannt werden.

Fazit

Durch SOC und SOCaMS wird das Cybersicherheitsniveau eines Unternehmens auf ein neues Level gehoben. Vorfälle und Schwachstellen werden

Einige Anbieter von EDR-Produkten (Endpoint Detection and Response)

Anbieter	Produkt	Link
Bitdefender	Gravity Zone	https://www.bitdefender.de/business/smb-products/advanced-business-security.html
CrowdStrike	Falcon	https://www.crowdstrike.de/endpoint-security-produkte/falcon-plattform/
DriveLock	Endpoint Detection & Response	https://www.drivelock.de/endpoint-detection-response-plattform-mehr-als-nur-protection
Kaspersky	Endpoint Detection and Response	https://www.kaspersky.de/enterprise-security/incident-response
McAfee	MVISION DER	https://www.mcafee.com/enterprise/de-de/products/mvision-edr.html
Microsoft	Defender Advanced Threat Protection	https://www.microsoft.com/de-de/microsoft-365/windows/microsoft-defender-atp
Palo Alto	Cortex XDR	https://www.paloaltonetworks.de/cortex/cortex-xdr
Trend Micro	XDR	https://www.trendmicro.com/de_de/business/products/detection-response/xdr.html
Varonis	Threat Detection & Response	https://www.varonis.com/solutions/threat-detection-response/
VMware	Carbon Black Cloud	https://www.carbonblack.com/resources/vmware-carbon-black-cloud-endpoint-protection-that-adapts-to-your-business/

viel schneller erkannt und der Umgang damit erleichtert. Gänzlich verhindern können sie Hackerangriffe aber nicht, da sie trotz der Schwachstellenanalyse oft nur reaktiv arbeiten. Durch das grundsätzlich asymmetrische Setting zwischen Angreifer und Verteidiger sind Angreifer immer im Vorteil. Eingesetzte KI- oder Machine-Learning-Anwendungen können zwar immer mehr Daten filtern und Angriffe erkennen und abwehren, einen 100-prozentigen Schutz können aber auch sie nicht bieten. Daher gilt es auch hier, angesichts begrenzter Ressourcen abzuwägen, inwiefern eine Anschaffung solcher eigener Tools sinnvoll ist oder ob diese über externe Anbieter genutzt werden. Auch Lösungen in der Cloud bieten hier Vorteile hinsichtlich der Skalierbarkeit und Flexibilität.

Dennoch ist der proaktive Umgang mit dem Thema Cybersicherheit für alle Unternehmen ein Muss. Alle digitalen Abläufe, Systeme und Daten müssen ständig überwacht und angepasst werden. Durch frühzeitige Reaktionen kann man viele Risiken umgehen und abmildern und so viel Geld sparen. SOCs und SOCaMS können dies sehr gut leisten. Letztlich ist es weniger entscheidend, welcher Ansatz oder welche Kombination gewählt wird, sondern dass es auch ordentlich funktioniert, schnell zu implementieren und zu skalieren ist. Hierbei ist es wichtig, sich von dogmatischen Sichten wie „Unsere Daten sind so vertraulich, die behalten wir nur intern und on Premises“ zu lösen und rein objektive Betrachtungen vorzunehmen. (ur@ix.de)

Hans-Wilhelm Dünn
ist Mitbegründer und seit 2018 Präsident des Cyber-Sicherheitsrats Deutschland e. V. Als Fachautor ist er u. a. Mitherausgeber des Standardwerks „Cybersicherheit im Krankenhaus“.

Unvorbereitet

Videokonferenz-Dienstleister im Datenschutztest

In den ersten Monaten der Coronapandemie lernte nahezu jede und jeder praktisch aus dem Nichts, mit zahlreichen Videokonferenztools umzugehen. Datenschutzaspekte wurden zumeist um der Kommunikation und der guten Zusammenarbeit willen vernachlässigt.

Im Zuge der Coronapandemie mussten plötzlich nicht nur zahlreiche Homeoffice-Arbeitsplätze her, sondern auch Videokonferenztools, um die Menschen in ihren Homeoffices zu vernetzen. Datenschutz und technische Sicherheit wurden dabei oft nicht beachtet. Ein Test der Berliner Datenschutzbeauftragten von Systemen aus der Cloud (siehe ix.de/zf6b) zeigt die Mängel deutlich.

Vielfach haben Unternehmen für ihre Videokonferenzen einfach „irgendwas“ genommen. Datenschutzrechtliche Fragen? Technische Sicherheit? Wurden oft schlicht übersehen oder ignoriert. Dabei bestehen in beiden Bereichen besonders große Risiken, wenn die Videokonferenzlösung nicht selbst betrieben, sondern als Dienst eingekauft wird: Was macht der Anbieter mit den Daten, die über die Leitung gehen? Was macht er mit den Informationen über die an den Konferenzen Teilnehmenden? Und wenn eine spezielle Software für die Nutzung nötig ist – telefoniert die vielleicht auch nach Hause?

Das Gesetz sagt: Erst prüfen, dann handeln

Die Datenschutz-Grundverordnung (DSGVO) stellt hohe Anforderungen an den Einsatz von Dienstleistern, sobald personenbezogene Daten ins Spiel kommen. Das ist bei Videokonferenzen immer der Fall, weil Sprache und Bild der Teilnehmenden verarbeitet werden, oftmals auch deren Kontaktdaten und Daten weiterer Personen, über die gesprochen wird.

Deshalb verlangt das Gesetz, dass nur Dienstleister mitspielen dürfen, bei denen sichergestellt ist, dass sie sich an die DSGVO halten. Und das Unternehmen, das Videokonferenzdienste nutzen möchte, muss einen Auftragsverarbeitungsvertrag mit dem Anbieter abschließen. Verschiedene Mindestanforderungen schreibt Artikel 28 DSGVO vor. Insbesondere darf der Anbieter die personenbezogenen Daten nur auf Weisung des Kundenunternehmens verarbeiten. Will der Anbieter die Daten außerhalb der EU oder des Europäischen Wirtschaftsraums verarbeiten, darf dadurch das Datenschutzniveau nicht nennenswert verringert werden. Die DSGVO sieht daher für solche Datenexporte zusätzliche Anforderungen vor, die meist durch den Abschluss der von der EU-Kommission beschlossenen Standardvertragsklauseln erfüllt werden sollen.

Was Unternehmen also auf der technischen Seite einsparen, wenn sie ihr Videokonferenztool nicht selbst betreiben, wird auf der rechtlichen Seite zu einem guten Teil wieder zunichtegemacht, weil die verschiedenen Verträge und Dokumente des Anbieters geprüft werden müssen. Die Anforderungen sind komplex, jeder Anbieter kocht sein eigenes Süppchen, und die meisten versuchen an verschiedenen Stellen, den Vertrag möglichst weit zu ihren Gunsten zu drehen. Solche Prüfungen sind daher sehr aufwendig.

Außerdem muss der Auftraggeber auch die technische Sicherheit beim Anbieter prüfen, denn er ist für alles verantwortlich, was dort passiert. Der Auftraggeber muss auch nachweisen können, dass sowohl er selbst als auch sein Dienstleister das Gesetz einschließlich der nötigen Sicherheit einhalten. Dabei helfen bei größeren Anbietern Auditberichte spezialisierter Firmen. Doch muss auch bei diesen Auditberichten geprüft werden, ob sie wirklich alle erforderlichen Sicherheitsnachweise liefern.

Datenschutzbehörde prüft schon mal vor

Um besonders kleineren Unternehmen, Vereinen und Behörden, die nicht über spezialisierte Rechts- und IT-Abteilungen verfügen, zu helfen, hat die Berliner Datenschutzbeauftragte in einem ersten Schritt die Auftragsverarbeitungsverträge verschiedener Videokonferenzanbieter geprüft (siehe Kasten „Der Test der Berliner Datenschutzbeauftragten“). Sollen die Daten auch in Drittländern verarbeitet werden, haben sich die Datenschützer auch die dafür vorgesehene Rechtsgrundlage angeschaut.

Kam ein Anbieter ohne größere Blessuren durch die rechtliche Prüfung, folgte eine technische Prüfung auf einige grundlegende Anforderungen – etwa auf die Schlüssigkeit der Anbieterangaben zur Verschlüsselung, auf einfache Angriffsmöglichkeiten wie Man in the Middle und auf Gestaltungsfragen mit datenschutzrechtlicher Relevanz: Ob etwa Kamera und Mikrofon der Teilnehmenden standardmäßig eingeschaltet sind oder gar aus der Ferne aktiviert werden können. Auch wenn die Aufsichtsbehörde betont, dass die Listen der gefundenen Mängel nicht abschließend sind – lang sind sie. Bei Microsoft Teams kommt dazu noch, dass der Auftragsverarbeitungsvertrag „an vielen Stellen unklar und widersprüchlich“ ist. Diese Kritik an dem Vertragswerk ist von besonderer Bedeutung, weil Microsofts „Online Service Terms“ und der „Anhang zu den Datenschutzbestimmungen für Microsoft-Onlinedienste“ für fast alle professionellen Microsoft-Produkte gelten, darunter Microsoft 365, früher bekannt als Office 365. Die Berliner Datenschutzbeauftragte zeigt sich am Ende ihrer Ausführungen zu Teams auch irritiert darüber, dass Microsoft den Auftragsverarbeitungsvertrag still nachträglich geändert hat. Kunden müssen nun damit rechnen, dass die Aufsichtsbehörde spezifisch auch prüft, ob denn die Verträge überhaupt formgerecht abgeschlossen worden sind und der Auftraggeber nachweisen kann, was der Vertragsinhalt ist.

Konkrete Kritik erntet Microsoft – wie auch Blizz und Cisco – dafür, dass sich das Unternehmen vorbehält, die im Auftrag verarbeiteten Daten auch zu eigenen Zwecken zu verarbeiten.

Unter den Anbietern, die „rote Ampeln“ erhielten, ist es weit verbreitet, die Pflichten des Anbieters und die Rechte des Kunden stärker einzuschränken, als das Gesetz es erlaubt. Aus der Weisungsbindung des Anbieters als Auftragsverarbeiter folgt etwa, dass dieser die Daten löschen muss, wenn sein Auftrag erledigt ist. Von diesem Grundsatz lässt die DSGVO nur wenige Ausnahmen zu. Auch wenn unklar bleibt, ob die Anbieter damit unbekannte Zwecke verfolgen, ob sie keine vernünftigen Löschroutinen umsetzen können oder wollen oder ob sie einfach nur schlampige Verträge machen – dass ihre Löschpflichten nicht ausreichen, mussten sich Cisco WebEx, die Telekom mit ihrem WebEx-Angebot, Google

Der Test der Berliner Datenschutzbeauftragten

Die Berliner Datenschutzbeauftragte hat Videokonferenzen aus der Cloud geprüft – und allen getesteten großen Anbietern ein schlechtes Zeugnis ausgestellt (einen Ausschnitt daraus zeigt die Abbildung): Blizz, Cisco WebEx, Google Meet, GoToMeeting, Microsoft Teams, Skype, Skype for Business Online und Zoom müssen sich mit einer roten Ampel zufriedengeben.

Cisco WebEx über die Telekom kam auf eine gelbe Ampel, weil der Dienst zwar zum Testzeitpunkt nicht legal nutzbar war, aber die Datenschützer vermuten, dass die Mängel „ohne wesentliche Anpassungen der Geschäftsabläufe und der Technik" beseitigt werden können. Grüne Ampeln auf der rechtlichen Ebene erhielten neben Tixeo und Wire verschiedene Anbieter von Jitsi- und BigBlueButton-Installationen.

Auf der technischen Ebene war die Aufsichtsbehörde mit keinem Anbieter hundertprozentig glücklich: Eine Freigabe der Standardkonfiguration für Videokonferenzen mit hohem Schutzbedarf erhielt nur Wire. Bei jedem Dienst verlangen die Datenschützer zudem kleinere Konfigurationsänderungen und Ähnliches. Zwischenzeitlich haben die meisten Anbieter angekündigt, die Kritik der Berliner Datenschutzbeauftragten aufgreifen zu wollen.

Zusätzlich gibt es weitere Empfehlungen und eine Checkliste zu Videokonferenzen allgemein und Hinweise, wenn ein Unternehmen selbst die Vertragsdokumente eines Anbieters prüfen will oder muss (sie sind über ix.de/zf6bzu finden).

Berliner Beauftragte für Datenschutz und Informationsfreiheit

Quelle: BlnBDI

R	T	Dienst	URL	Version der Dokumente	Rechtliche Mängel bzgl. Auftragsverarbeitung	Ort der Verarbeitung nach Vertrag auf EU/EWR beschränkt
		Blizz	https://www.blizz.com/de/	Blizz Auftragsverarbeitungsvertrag (https://www.blizz.com/de/auftragsverarbeitungsvertrag/), Endnutzer-Lizenzvereinbarung – Blizz (https://www.blizz.com/de/eula/), jeweils ohne Datum, letzter Abruf 28.5.2020 [Deutsch]	ja, siehe Anmerkung Anbieter hat Änderungen angekündigt	nein
		Cisco WebEx	https://www.webex.com/de	Universelle Cloud-Vereinbarung Version 9.3 vom 15.4.2020 [Deutsch]; Master Data Protection Agreement, Dezember 2019 [Englisch]; Digital River Ireland Ltd. Allgemeine Geschäftsbedingungen und Verbraucherinformationen Deutschland vom 24.7.2017 [Deutsch]	ja, siehe Anmerkung	nein
		Cisco WebEx über Telekom	https://konferenzen.telekom.de/produkte-und-preise/telefon-und-web/cisco-webex/	Auftragsverarbeitungsvertrag zum Vertrag über Cisco Webex (Webex Standard) Version 1.0 vom 15.01.2020 [Deutsch], Anhang AVV zum Vertrag über Telekom Kollaborationsleistungen Version 2.2 vom 16.04.2020 [Deutsch]	ja, siehe Anmerkung Anbieter hat Änderungen angekündigt	nein, siehe Anmerkung
		frei verfügbare Jitsi-Angebote			in der Regel ja, da kein Auftragsverarbeitungsvertrag	

Nur wenige Anbieter von Videodiensten erhielten eine grüne Ampel im Kurztest der Berliner Datenschutzbeauftragten – hier ein Ausschnitt aus der Tabelle.

Meet und Zoom vorwerfen lassen. Microsoft hat diesen Mangel zwar bei seinem „stillen Update" seines Auftragsverarbeitungsvertrags behoben, dafür aber neue Abweichungen vom gesetzlichen Mindeststandard eingefügt.

Natürlich will kein Rechenzentrumsbetreiber Vor-Ort-Kontrollen von Tausenden Auftraggebern haben. Aus Sicherheitsgründen sind solche Kontrollen auch höchst unerwünscht. Doch die DSGVO sagt: Der Auftraggeber ist für alles haftbar, was der Dienstleister macht, und er muss zumindest das Recht haben, zu überprüfen, ob alles in Ordnung ist. Hierfür muss der Dienstleister seinem Kunden alle notwendigen Informationen zum Nachweis bereitstellen. Außerdem muss er dem Kunden oder seinem Beauftragten erlauben, Vor-Ort- und andere Kontrollen vorzunehmen. Der sowohl aus sicherheitstechnisch-organisatorischer wie rechtlicher Sicht richtige Ansatz ist daher, dass der Anbieter einen über alle Zweifel erhabenen unabhängigen Dritten mit einem Audit beauftragt. Ideal wären dafür Datenschutzzertifizierungen, wie sie die DSGVO ausdrücklich vorsieht – doch leider gibt es noch keine entsprechenden Zertifizierungen.

Versuche, die Kontrollrechte einzuschränken oder auszuschließen, monieren die Datenschützer bei Blizz, WebEx über Telekom, Google Meet, GoToMeeting, Microsoft Teams und Zoom, wobei sich die Kritik bei Blizz, WebEx über Telekom und Google Meet darauf beschränkt, dass Audits des Kunden auch dann kostenpflichtig sind, wenn sie ausschließlich durch Pflichtverletzungen des Anbieters notwendig geworden sind. Bei Blizz, WebEx über Telekom, Google Meet, GoToMeeting und Zoom kritisiert die Datenschutzbeauftragte zudem, dass der Vertrag die Pflicht des Anbieters, Informationen zum Nachweis seiner Compliance bereitzustellen, unzulässig beschränkt.

Datenexporte vor und nach Schrems II

Die Version 1.0 der Videokonferenzanbieterliste hat die Berliner Datenschutzbeauftragte noch vor Schrems II veröffentlicht – jenem Urteil des Europäischen Gerichtshofs vom 16. Juli 2020, das Übermittlungen personenbezogener Daten an IT-Dienstleister in den USA weitgehend unmöglich macht, weil dort die Grundrechte europäischer Bürgerinnen und Bürger missachtet werden. Und doch kam die Behörde schon vor Schrems II zu dem Schluss, dass die von vielen großen Anbietern vorgesehenen Datenexporte in die USA und andere Drittstaaten illegal sind.

Manche Anbieter wie Cisco ersparen sich gleich so lästige Fragen wie die nach den Standardvertragsklauseln und setzen von vornherein auf illegale Datenexporte, Google schließt die Standardvertragsklauseln nur auf Verlangen des Kunden ab. Andere wie GoToMeeting, Microsoft Teams und Zoom schränken ihre Pflichten aus den Standardvertragsklauseln ein, womit diese dann nicht mehr als Erlaubnis für den Datenexport taugen. Immerhin „nur“ als unklar in Sachen Datenexporte – und damit erst einmal „nur“ als ein Verstoß gegen das sogenannte Accountability-Prinzip aus Artikel 5 Absatz 2 DSGVO, wonach alle Datenverarbeitungsverantwortliche nachweisen müssen, dass sie das Gesetz einhalten – kommen die Auftragsverarbeitungsverträge von Blizz und Cisco WebEx sowie die Telekom weg.

Nach Schrems II wird die Sache mit den Datenexporten nun noch komplizierter. Denn die Standardvertragsklauseln regeln nur den zivilrechtlichen Teil der erforderlichen Garantien für den Datenexport. Ob im Zielland die Behörden nach europäischem Maßstab unzulässige Zugriffsrechte auf die Daten haben und ob sich die Betroffenen dagegen vor Gericht wehren können, müssen Kunde und Anbieter selbst prüfen – und nachweisen, dass das Datenschutzniveau ausreicht. Allein der damit verbundene Aufwand spricht dafür, künftig personenbezogene Daten nur noch in Ländern zu verarbeiten, die der EU oder dem EWR angehören oder für die die EU-Kommission verbindlich festgestellt hat, dass sie ein angemessenes Datenschutzniveau haben. Nach dem „Schrems II“-Urteil scheiden jedenfalls diejenigen Videokonferenzdienste aus, die die Daten auch in den USA verarbeiten. Denn zwar verschlüsseln einige (wenige) Anbieter die Inhalte Ende zu Ende. Doch bei den Metadaten, also etwa, wer mit wem kommuniziert, ist das technisch nicht möglich.

Empfehlungen

Wer Komfort und Verbindungsqualität der großen US-Anbieter gewöhnt ist, wird die Empfehlungen der Berliner Datenschutzbeauftragten bitter finden: Am besten die Videokonferenzlösung selbst betreiben. Wenn das nicht geht, einen Anbieter wählen, der die Daten nur in der EU, dem EWR oder einem von der EU-Kommission als datenschutzrechtlich angemessen anerkannten Land verarbeitet – also auf die meisten bekannten Anbieter verzichten. Der Anbieter muss dann eine ausreichende Sicherheit, etwa durch eine Zertifizierung, nachweisen, eine Verschlüsselung der Daten garantieren und einen ordnungsgemäßen Auftragsverarbeitungsvertrag abschließen. Und natürlich seine Finger von den Nutzerdaten lassen. Da die Standardkonfigurationen leider oft gegen die DSGVO verstoßen, sind vor der ersten Nutzung zudem meist noch Konfigurationsänderungen nötig. Datenschutzkonforme Angebote gibt es durchaus auf dem Markt, wie die grünen Ampeln zeigen. (ur@ix.de)

Quellen

Die Dokumente der Berliner Datenschutzbeauftragten sind über ix.de/zf6b zu finden.

Matthias Bergt
leitet das Referat I B (Recht) bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit und ist damit für den größten Teil der Berliner Unternehmen zuständig.

Teure Agilität

Sicherheit für Container

Allzu häufig wird die IT-Sicherheit vernachlässigt, das ist bei Containern nicht anders als im Rest der (IT-)Welt. Wie kann man es besser machen und die Sicherheit von Anfang an einbeziehen?

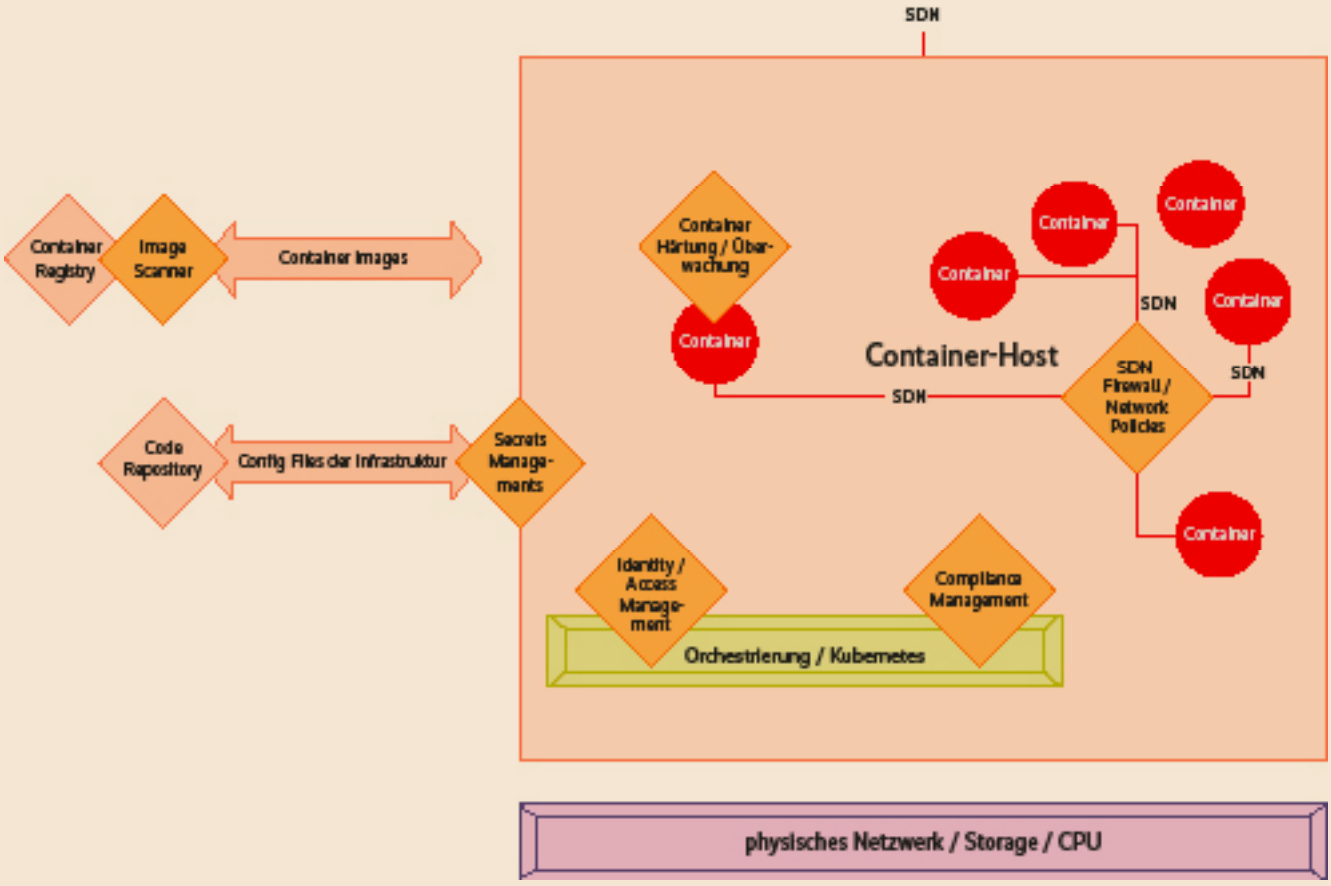
Agile IT und Container bringen immense Vorteile. Leider wird das, was dauert und was kostet, ohne einen direkt ersichtlichen oder messbaren Nutzen zu bringen, häufig nicht beachtet: die Sicherheit der Infrastruktur und auch der Anwendungen in der schönen neuen Container-Welt. Zu viele DevOps-Teams vergessen, die Absicherung in ihre agile Kultur mit einzubauen.

Hier helfen DevSecOps, also die Integration von Sicherheit in den Entwicklungsprozess von Anfang an, und das von Google entwickelte Site Reliability Engineering (SRE) mit dem Ziel der Sicherstellung des täglichen Betriebs und als Regelwerk für auftretende Störungen. Die Grundpfeiler für eine agile und sichere Entwicklung und den Betrieb sind:

- Standardisierung und Automatisierung: Manuelle Veränderungen sollten nicht vorkommen, so reduziert sich die Wahrscheinlichkeit von unabsichtlichen Fehlern.
- Scans des Codes und der Images: In jeder Phase ist das Einhalten von Sicherheitsvorgaben automatisiert zu kontrollieren und dies fest in die Pipelines einzubauen.
- IAM (Identity and Access Management) und RBAC (Role-based Access Control): Identitätsmanagement und rollenbasierte Rechte nicht nur für Personen, sondern auch für alle Prozesse.
- Separierung und Abgrenzung: Zwischen Prozessen, Services und mindestens der Verwaltung der Umgebungen ist eine ausreichende Sicherheitsgrenze zu ziehen;
- Schnelle Patches: Jedes Image und jeder Server muss ständig und umgehend neue Versionen erhalten können.

Vertrauen ist gut, Monitoring besser

Grundlegend geändert hat sich hier das Monitoring auf Verfügbarkeit. Früher wurde gemessen, ob ein Prozess läuft oder ein Port offen ist, und wer gut war, hat die Anwendung einen Statuscode ausgeben lassen. Heute erwarten alle, dass Anwendungen immer laufen und dass sie immer antworten. Die Herausforderung jetzt ist die Geschwindigkeit der Antwort und ob diese auch den Erwartungen entspricht. Der Betrieb hat sich weiterentwickelt zu einer umfassenden Überwachung aller Anfragen auf Korrektheit und Latenz. Google hat mit SRE hier neben dem be-



Ein Orchestrierungstool wie Kubernetes verwaltet und steuert den Einsatz zahlreicher Sicherheitswerkzeuge, die an unterschiedlichen Ebenen ansetzen.

kannten Service Level Agreement (SLA) noch die Service Level Objective (SLO) und den Service Level Indicator (SLI) festgelegt. Beide definieren die Messung der Verfügbarkeit und sind nicht auf „an“ oder „aus“ beschränkt.

Der zweite Aspekt des Monitorings ist die Überwachung, ob Sicherheitsvorgaben eingehalten werden. Moderne Betriebsumgebungen sind aus vielen Schichten aufgebaut, und auf jeder Schicht gibt es Hunderte von Einstellungen, die die Sicherheit beeinflussen.

Hier wie überall sonst ist Automatisierung notwendig, um diese Einstellungen zu überwachen, Fehler zu beheben und sie über alle Betriebsstätten hinweg im Blick zu haben.

Wer seine Anwendungen nicht nur im eigenen Rechenzentrum auf vielen Clustern und Umgebungen hat, sondern auch in der Virtual Private und der Public Cloud betreibt, hat schnell Dutzende unterschiedlicher Benutzeroberflächen zu bedienen, um die aktuelle Sicherheit zu auditieren.

Werkzeuge zum Compliance-Management helfen hier sehr gut weiter und sind in größeren Umgebungen die einzige Chance, den Überblick zu behalten. Auch wenn diese Themen in der „alten“ Welt ohne Container schon relevant waren – mit Containern steigt die Flexibilität, die Betriebsumgebungen sind um Größenordnungen komplexer, und somit ist die Notwendigkeit der Automatisierung solcher Überwachungsvorgänge noch dringlicher.

Mächtige Werkzeugkästen im Einsatz

Das Compliance-Management ist teilweise auch in den verfügbaren Werkzeugkästen für die Absicherung der Container und ihrer Betriebsumgebungen enthalten. Oft sind spezialisierte Werkzeuge da noch etwas umfassender, aber zumindest ein Abgleich aller Einstellungen mit den Vorgaben der Sicherheits-Benchmarks des Center for Internet Security (CIS) ist eigentlich in allen enthalten. Das CIS erstellt sehr umfangreiche Listen mit technischen Vorgaben, die zumeist die Konfiguration der Dienste betreffen. Diese sind meist mehrere Hundert Seiten lang und ein manueller Abgleich ist sehr mühselig. Um eine ständige Überwachung der Sicherheit zu ermöglichen, sollte diese Aufgabe für alle Betriebsumgebungen automatisiert sein.

Wer die Werkzeugkästen und die spezialisierten Tools der Containerabsicherung verstehen will, muss wissen, dass Container und das damit heute fast immer mit im Einsatz befindliche Orchestrierungstool Kubernetes (K8S) nicht einfach eine andere Art sind, einen Prozess zu starten, sondern dass K8S eigentlich den gesamten RZ-Betrieb übernimmt. Es steuert die softwaredefinierten Netzwerke, verwaltet die Firewallregeln in diesen Netzwerken, überwacht die Anwendungen, startet und stoppt die Prozesse, verlagert Prozesse von ausgefallenen Servern auf andere, und wenn es zu wenige Server sind, bestellt es gleich noch welche dazu.

Auch steuert Kubernetes die Speicher-Backends und weist den Speicher den Anwendungen zu. Allerdings ist K8S eher der Vermittler zwischen einer Vielzahl an Werkzeugen, die jeweils einen Job erfüllen.

Unter der Haube von K8S arbeiten Dutzende Tools zusammen, die speichern, wie die Umgebung aussehen soll, verifizieren, dass der Nutzer ausreichende Rechte hat, den aktuellen Stand überwachen und den gewünschten Zustand wiederherstellen.

Und genau da setzen diese Multi-Tools an. Zumeist übernehmen sie drei wichtige Grundfunktionen:

- das Überwachen von Netzwerkregeln;
- das Überwachen von Verhaltensregeln wie SECCOMP und APPArmor oder SELinux;
- das Erzwingen von Compliance-Monitoring der Server und der Container sowie von K8S selbst.

Teilweise ist noch die Überwachung und die Reaktion auf Sicherheitsverstöße mit enthalten, wobei hier der Fokus der einzelnen Produkte etwas unterschiedlich ist. Manche sind eher aus dem Prozessmonitoring und mit Host-based Intrusion Detection vergleichbar, während andere mehr die Netzwerkthemen inklusive Network-based Intrusion Detection bedienen.

Allen gemeinsam ist jedoch, dass sie über eine rein passive Überwachung hinausgehen und bei Vorfällen auch eingreifen, indem sie beispielsweise verdächtige Prozesse beenden, Netzwerkregeln anpassen und Container neu starten, um den Angreifer nicht weiter vordringen zu lassen. Sie gehen sogar bis hin zur Automatisierung der Forensik, indem sie bei Vorfällen alle Daten sammeln, die für die Aufklärung durch einen Menschen hilfreich sein können.

Rechtliche Vorgaben

Für viele Organisationen stellen die Richtlinien der Kreditkartenindustrie (PCI), die KRITIS-Verordnung oder das Grundschutz-Kompendium des BSI rechtlich verbindliche Vorgaben oder zumindest starke Empfehlungen dar, mit denen sie die Absicherung der Daten auch in Sachen Datenschutz nachweisen können. Hier hat das BSI immerhin schon vor drei Jahren den ersten Entwurf eines Bausteins für den Betrieb von Containern zur Kommentierung gestellt und Anfang dieses Jahres stark überarbeitet (siehe ix.de/zfaq). (ur@ix.de)

Quellen

Der Community Draft des BSI zur Absicherung von Containern ist unter ix.de/zfaq zu finden.

Christoph Puppe
ist Security Consultant bei SVA, Auditteamleiter für ISO 27001 nach Grundschutz, Mitautor des Grundschutz-Kompendiums und ehemaliger Penetrationstester.