Live
Blue Boy Show
04.03.2020 | 18:00

CSF MAGAZIN

DAS OFFIZIELLE PROGRAMMHEFT ZUM CYBER SECURITY FAIREVENT

CSF Cyber Security Fairevent

Messe | Event | Kongress | Erlebniswelt

Dortmund, 04.–05. März 2020

SICHER IM CYBERSPACE

Das Cyber Security Fairevent in Dortmund

Wertvolle Kontakte knüpfen
Innovative Cyber-Security-Unternehmen
Top Keynote Speaker aus der Praxis

Weitere Informationen zum CSF finden Sie im Heft!

FOR PROFESSIONALS ONLY

WAVELINE-MAR.COM

WERBEAGENTUR & MESSEDESIGN

Marketing

Advertising

Events / Fairs
EMEA wide Event Support

Creation / Graphic Design /
Project Management

Fulfillment

www.waveline-mar.com

Editorial

Willkommen zum CSF!

Worauf müssen sich CISOs 2020 einstellen, was werden sich Cyberkriminelle im neuen Jahr einfallen lassen und wie sicher sind wir im neuen Jahrzehnt? Man möchte wirklich nicht in der Haut der CISOs stecken, nur das ist sicher.

Aber aufgeben ist nicht drin. Schließlich gibt es innovative IT-Security-Unternehmen, die z. B. mit Unterstützung der künstlichen Intelligenz, immer besseren Lösungen, Awareness-Schulungen, Zertifizierungen bis hin zu den immer noch zuverlässigen Magnetbändern Cyberkriminellen erfolgreich den Kampf angesagt haben.

Ich bin stolz, einige dieser innovativen Unternehmen beim CSF als Aussteller begrüßen zu können. Beim CSF präsentieren wir nicht „nur“ Lösungen, sondern mit „The Best of Both Worlds“ auch ein neues Veranstaltungskonzept, das Bewährtes aus Messen und Events vereint und mit neuen Ideen und Impulsen, wie etwa den Solution Panels und dem Matching-Tool für Angebot-und-Nachfrage zur nachhaltigen Geschäftsanbahnung, begeistern wird.

An dieser Stelle möchte ich mich bei allen Mitwirkenden, Mitarbeitern, Partnern, Institutionen, Medienpartnern, Ausstellern und Keynote Speakern bedanken und Sie alle zum Cyber Security Fairevent an einem Top-Termin in NRW, in einer Region mit viel Potenzial und dem vielversprechenden Standort in Dortmund einladen. Ich freue mich schon, Sie beim CSF zu begrüßen. Ihr persönliches Online-Gastticket erhalten Sie mit diesem QR-Code.

Hasan Ezdi
Founder/Business Owner
Cyber Security Fairevent &
Waveline-Mar.Com

Vielen Dank an unsere Medienpartner

COMPUTERWELT · CRN · DCI · DIGITAL BUSINESS CLOUD
DIGITAL ENGINEERING · DIGITAL MANUFACTURING · DIGITAL PROCESS INDUSTRY · funkschau
gi GELDINSTITUTE · it-daily.net · itmanagement · itsecurity
kes · LANline · Markt&Technik · SICHERHEIT. DAS FACHMAGAZIN.
SecuPedia · Ihr Systemhaus · manage it · vb

Acronis

DIGITALE WERTE BENÖTIGEN CYBER PROTECTION

Schützen Sie Ihre Daten vor Cyber Crime und Daten-verlusten dank der innovativen Acronis Cyber Protection.

Besuchen Sie unsere Vorträge im Forum Business Solutions und unseren Stand, um mehr zu erfahren.

www.acronis.com

Inhalt

Die CSF-Themen

Die CSF-Aussteller

Gastbeiträge der Medien- und Kooperationspartner

Rubriken

*Teilnehmende Aussteller**

Acronis · ALTARO · avast business · corelight · CROWDSTRIKE · BlackBerry CYLANCE · datto · DQS THE AUDIT COMPANY · eset ENJOY SAFER TECHNOLOGY · F-Secure · G DATA TRUST IN GERMAN SICHERHEIT · indevis · ixia A Keysight Business · kaspersky · OneTrust Privacy · RAPID7 · SentinelOne · SOPHOS · TELONIC · tenable · TUXGUARD · VARONIS · WatchGuard

Kooperationspartner

me · h&g EDITORS · it-club dortmund unna hamm · DIGITALE WOCHE DORTMUND · forward.now marketing-service · IT&DATA

** Teilnehmer bei Redaktionsschluss*

Wir stellen vor

Die Moderatoren und Keynote Speaker des CSF

Unsere erfahrenen Keynote Speaker sprechen auf der CSF Stage über Ihre Praxiserfahrungen aus der Technologie-, Versicherungs- und Verlagsbranche, der Chemie-/Pharmaindustrie, der Rechtsberatung sowie des Landeskriminalamtes NRW.

Saskia Naumann

Moderatorin & Journalistin

Moderation

Holger Berens

Vorstand BSKI e.V.
Leiter KIS an der RFH

Moderation

Peter Vahrenhorst

Kriminalhauptkommissar

Prevention Cybercrime
Landeskriminalamt
Nordrhein-Westfalen

04.03.2020 | 09:30 Uhr

Florian Jörgens

Chief Information Security Officer (CISO)
Lanxess Deutschland GmbH

04.03.2020 | 11:00 Uhr

Matthäus Hose

Verlagsleiter/Publisher
WEKA FACHMEDIEN GmbH

04.03.2020 | 12:00 Uhr

Karin Tresp

Leitung
Datenschutz-Management
REWE Group (Z WSD)

04.03.2020 | 12:30 Uhr

Dr. Mathias Dehm

Head of Security & Privacy
Research & Governance
Continental AG

04.03.2020 | 13:20 Uhr

Burkhard Fertig

Leiter Organisation und IT
Suffel Fördertechnik
GmbH & Co. KG

04.03.2020 | 15:20 Uhr

Dr. Thomas Lapp

Rechtsanwalt
IT-Kanzlei dr-lapp.de GbR
und Vorsitzender NIFIS e.V.

04.03.2020 | 16:40 Uhr

Stephan Engel

Chief Cybersecurity Officer
Siemens AG

05.03.2020 | 11:10 Uhr

Olaf v. Wackerbarth

Senior Director
Cybersecurity (Global)
GE Healthcare

05.03.2020 | 12:20 Uhr

Stephan Gerhager

Chief IT Security Officer
Allianz Deutschland AG

05.03.2020 | 13:20 Uhr

Jörg Steinhaus

Konzerndatenschutz-
beauftragter Merck KGaA

05.03.2020 | 15:00 Uhr

Dr. Hans-Joachim Popp

Vorsitzender des Präsidiums
VOICE e.V.

05.03.2020 | 16:00 Uhr

Livehacking

Georg Jobst
IT Security Analyst
NSIDE ATTACK LOGIC GmbH

Erster Slot:
04.03.2020 | 10:00 Uhr

Aktuelle Agenda CSF Stage:

Agenden Foren Business Solutions Technical Solutions

ALTARO BACKUP

HYPER-V | VMWARE | PHYSICAL | OFFICE 365

Schnell. Leistungsfähig.
Erschwinglich.
Backup-Lösungen für die Sicherung von Microsoft Hyper-V-, VMware- & Office 365-Umgebungen.

Warum noch länger für überflüssige Funktionen zahlen?

Wir lassen Unnützes und Lästiges weg, um Ihnen eine agile, schlanke Lösung zu bieten...

Stressfrei und effizient

Exzellenter Support
Reaktionszeit unter 30 Sekunden

Unschlagbares Angebot

Testen Sie uns 30 Tage: www.altaro.com/de

ALTARO

www.altaro.com
sales@altaro.com
Tel: +49 (89) 20802-6955

vmware PARTNER TECHNOLOGY ALLIANCE

Microsoft Partner Gold Application Development

Autorisierter Partner

Gastbeitrag

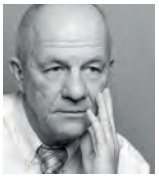
Neue Dimensionen im Hase-und-Igel-Spiel

Im Jahr 2019 identifizierte das BSI rund 400.000 neue Schadprogramme täglich, Tendenz steigend. Die Angriffsszenarien werden auch immer ausgeklügelter und besser, womit das Hase und Igel Spiel neue Dimensionen bekommt. Wie können die IT Abteilungen möglichst schnell Schadsoftware identifizieren? Das wird wohl zu einer der größten Herausforderungen für die CISOS in Unternehmen, da die Schutztechnologien teilweise veraltet und nicht up-to-date sind. Ein neues Problem ist in diesem Zusammenhang auch die Malware, die nicht an ausführbare Dateien gebunden ist und nahezu keine Spuren hinterlässt. Besonders Memory-based attacks stehen bei Hackern hoch im Kurs. Und wer erinnert sich nicht an den Trojaner Emotet, der 2019 etliche Unternehmen, öffentliche Verwaltungen und Universitäten infiziert hat? Dies wird sich auch im Jahr 2020 nicht ändern, da wirksame Endpoint-Protection-Maßnahmen in vorgenannten Institutionen immer noch nicht eingesetzt werden und es oft erst zum Schadensfall kommen muss, bevor in die Security investiert wird. Spätestens seit den groß angelegten, globalen Wanna-Cry- und NotPetya-Kampagnen wissen wir, dass ein weiteres Problem Ransomware ist und dies in den Griff zu bekommen, wird sich ebenfalls in 2020 nur schwer realisieren lassen. Ransomware-Attacken werden immer ausgefeilter und gezielter. So wird Ransomware nun schon speziell für diverse vertikale Märkte entwickelt, oder die Angreifer zielen auf besonders sensible Daten aus Forschung und Entwicklung.

Nicht erst seit der Einführung der DSGVO sind die Themen Cybersecurity und Datensicherheit in aller Munde. Die ständig wachsende Digitalisierung bringt zusätzlich eine immer größer werdende Menge aus persönlichen und geschäftlichen Daten hervor. Viele Unternehmen fokussieren sich dabei zu sehr auf die Gefahr von außen und vergessen die internen Risiken und deren Schadenspotenzial.

Obwohl weltweit die Bedrohungslage durch Hacker immer weiter zunimmt, ist ein Großteil der Unternehmen nicht in der Lage, Systeme und Daten effektiv zu schützen. Es klafft eine wachsende Lücke zwischen dem, was Unternehmen in Cybersicherheit investieren, und der Fähigkeit mit der Zahl der externen und internen Bedrohungen und auftretenden Datenschutzverletzungen Schritt zu halten. Es ist nicht die Frage ob, sondern nur wann man Opfer einer Datenexponierung wird. Umso alarmierender ist die Tatsache, dass die Mehrheit der Unternehmen die Sicherheitsbudgets für dieses Jahr entweder auf dem bisherigen Niveau einfrieren oder sogar senken wollen.

Wer wirklich von den Vorteilen der digitalen Transformation profitieren will, der muss sich klar machen, welche großen Risiken Firmen dadurch ausgesetzt sind. Unternehmen werden nicht umhin können, Cybersicherheit langfristig zu betrachten und sich von einem Sicherheitsansatz nach dem Motto „gerade noch gut genug“ zu verabschieden. Security by Design und Security by Default muss gelebte und sicher finanzierte Firmenstrategie werden.



Philipp Schiede

Geschäftsführer der ap Verlag GmbH manage it

www.manageit.de

RETHINK IT SECURITY.

CSF Cyber Security Fairevent

avast business
powered by AVG and Avast

Sicherheit muss intelligenter, einfacher zu verwalten und zuverlässiger denn je sein.

Lernen Sie Avast Business kennen.

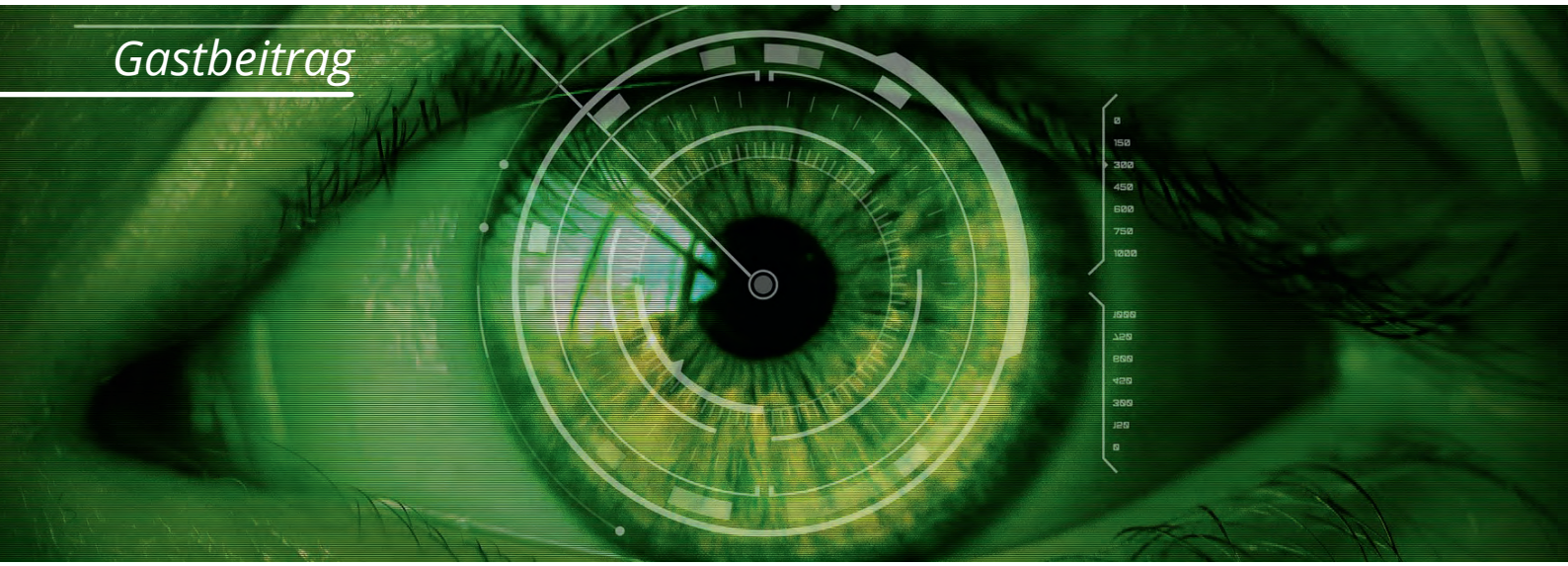
Avast schützt aktuell ca. 740.000 Unternehmen und ca. 435 Mio Endpoints weltweit.

Integrierte Managed Security Solutions für das moderne Business.

Avast Business bietet integrierte, Cloud-basierte Sicherheitslösungen für Endgeräte und Netzwerke zum Schutz von KMUs und IT-Dienstleistern. Das mehrstufige Sicherheitsportfolio von Avast Business stützt sich auf das größte und weiträumigste Netzwerk zur Bedrohungserkennung. Dadurch werden Schutz, Verwaltung und Überwachung von zunehmend komplexen IT-Umgebungen einfach und erschwinglich.

www.avast.com/business

Gastbeitrag



Kritischen Cyber-Bedrohungen intelligent begegnen

Cyberangriffe haben ein Ausmaß erreicht, das Banken vor immer größere Herausforderungen stellt. Früherkennung, schnelle Analyse von Sicherheitsrisiken und Präventionsmaßnahmen werden immer essenzieller. Vielen Banken fehlen jedoch die Ressourcen sowie oftmals auch ein umfassendes IT-Security-Know-how, um angemessen auf die Bedrohungen zu reagieren. Frank Reiländer, Head of Cybersecurity bei CGI, gibt im gi-Geldinstitute-Interview Antworten auf wesentliche Sicherheitsfragen.

Der Finanzsektor gehört zu den Top Angriffszielen von Cyberkriminellen. Wo liegen denn die Hauptrisiken für Banken?

Das wertvollste Asset der Banken ist aus Kundensicht das Vertrauen in die Sicherheit der Geldanlagen. Gleichbedeutend mit einem Banktresor vor 20 Jahren ist es heute wichtig, dass alle Daten in einem virtuellen Safe liegen und somit geschützt sind. Allerdings finden Cyberkriminelle immer neue Wege, welche die Finanzwirtschaft in gefährliche Bedrohungslagen bringen. Der klassische „Fraud“ – zu Deutsch „Betrug“ – stellt einen wesentlichen Teil der operationellen und Compliance-relevanten Risiken dar. Dieser kann sowohl durch externe als auch interne Betrugsversuche wie die Weitergabe von datenschutzrelevanten Informationen oder die Durchführung unzulässiger Insidergeschäfte stattfinden. Jedes mit dem Internet verbundene Gerät ist ein potenzielles Einfallstor und muss geschützt werden. Hinzu kommt der Faktor Mensch, der eine nur schwer zu beeinflussende Variable und somit ein Risiko darstellt. Fallen beispielweise durch erfolgreiche Angriffe Zahlungssysteme temporär aus oder werden Datenschutzverstöße begangen, kann dies fatale Auswirkungen haben. Insbesondere, wenn eine Bank den Cyberangriff erst verspätet bemerkt, kann dies ungeahnte Ausmaße annehmen.

Banken gelten als unzureichend geschützt. Gibt es beim Thema IT-Sicherheit aus Ihrer Sicht Fortschritte? Wird die Finanzbranche resistenter?

Nicht zuletzt aufgrund der zunehmend strengeren Meldepflichten nehmen Banken die gegebene Bedrohungslage ernst. Wurden früher Zwischenfälle meist intern gelöst, werden heute nicht zuletzt aufgrund der Pflicht, die Datenschutzbehörde zu informieren, sicherheitsrelevante Vorfälle bekannt. Diese führen nicht nur zu Imageschäden der betroffenen Bank, sondern auch dazu, dass neue Angriffsarten publik werden und Nachahmer anziehen.

Nach welchen Kriterien sollten Banken ihre Security-Lösungen auswählen?

Banken sollten ihre Security-Lösungen risikobewusst nach Kriterien der Nutzbarkeit und Wirksamkeit auswählen. Grundsätzlich ist zwischen internen und kundenbezogenen Lösungen zu unterscheiden. Nach außen hin sollte die Lösung das Gefühl der Sicherheit vermitteln, jedoch keine zusätzlichen Hürden wie Zusatzequipment, Registrierungen für Zertifikate oder Ähnliches aufweisen.

Herbert Sebald

Chefredakteur
gi Geldinstitute
geldinstitute.de

Cybersecurity that protects the complete attack surface with automated threat prevention, detection, and response capabilities. Learn more at cylance.com

BlackBerry | CYLANCE

Gastbeitrag

Dortmund – mit Sicherheit in die Smart City.

Standort mit Zukunft

Dortmund ist mit über 600.000 Einwohner*innen im westlichen Westfalen das Tor zur Rhein-Ruhr-Region im Herzen Europas. Dortmund ist eine Stadt des Mittelstands, der Technologie und der Dienstleistungen. Dortmund ist modern, leistungsfähig und lebenswert. Dortmund hat sich als innovativer Wissenschaftsstandort international einen Namen gemacht. So siedeln sich heute Zukunftsbranchen wie Informationstechnologien (IT), Mikro-/Nanotechnologie und zunehmend auch Biomedizin und Robotik an.

Wichtig für Dortmund ist dabei: Es geht nicht nur um die Technologie, sondern darum, dass sich die Menschen in der Stadt wohlfühlen. Es geht um eine zukunftsfähige – smarte – Stadt. Smart ist eine Stadt dann, wenn sie es schafft, die Lebensqualität der Menschen zu verbessern, den Wirtschaftsstandort zu stärken und dabei Infrastrukturkosten zu senken.

Allianz Smart City Dortmund – Wir.Machen.Zukunft.

Die Allianz Smart City Dortmund ist eine Initiative der Industrie- und Handelskammer zu Dortmund, der Stadt Dortmund, der Leitstelle Energiewende Dortmund (L.E.D.) und der Cisco Deutschland. Gemeinsam mit über 150 weiteren Allianzpartnern arbeiten wir daran, Dortmund zur Smart City zu machen, entwickeln Ideen und Projekte, akquirieren Fördergelder und setzen Maßnahmen um. Unsere Leitfrage: Wie kann unsere Stadt lebenswerter werden und einen besseren Service für die Bürgerinnen und Bürger sowie für die Unternehmen gewährleisten? Dafür nutzen wir bspw. intelligente Sensoren und eine breite Vernetzung der städtischen Infrastruktur und Akteure.

Sichere Nutzung von Daten und Einsatz von Technologien

Die technische Verbesserung der Infrastruktur wirft häufig auch moralische Fragestellungen oder Fragen zur (Daten-)Sicherheit auf, mit denen sich der Ombudsmann für Datenwert und Datenethik der Stadt Dortmund - Alexander von Schweinitz - beschäftigt.

Wer bekommt Zugriff auf die Daten einer Smart City? Welchen Wert haben Daten für eine Stadt und ihre Unternehmen? Wie sieht ein ethischer Umgang mit Daten aus und wie setzen wir die Daten zum Wohl unserer Bürger ein? Dies sind nur einige Beispiele für Fragen, denen sich zukünftig – noch viel stärker als bisher – die Kommunen in Deutschland stellen werden.

Die Allianz Smart City Dortmund ist eine Plattform, auf der innovative Lösungen für die Stadt der Zukunft entwickelt und getestet werden. Von Energie und Mobilität über Sicherheit und Facility-Management bis hin zu smarten Services im Quartier und der modernen Infrastruktur von morgen. Nutzen Sie als Unternehmen oder wissenschaftliche Einrichtung die Innovationskraft der Allianz Smart City Dortmund als Chance, die smarten Lösungen und Geschäftsmodelle für die Städte der Zukunft und natürlich auch für Dortmund zu entwickeln, zu erproben und nutzbar zu machen.

Sebastian Winkler

Geschäftsführung
Allianz Smart City
Dortmund


CROWDSTRIKE
BUILT
TO STOP
BREACHES
GEBEN SIE CYBER-ANGRIFFEN KEINE CHANCE!
CROWDSTRIKE FALCON SCHÜTZT SIE.
ERFAHREN SIE MEHR UNTER
crowdstrike.com/seedemo
WWW.CROWDSTRIKE.DE

Ransomware: Was MSPs gegen die Gefahr tun können

Die Cyber-Angriffe mit Malware wie Emotet auf deutsche Behörden, Krankenhäuser und KMU zeigen: Die Angreifer schlagen überall dort zu, wo Ausfallzeiten besonders schwerwiegende Konsequenzen haben. MSPs müssen sich gut rüsten, um die Sicherheit ihrer Kunden und ihrer eigenen Unternehmen gewährleisten zu können.

Bild: datto

Der aktuelle Ransomware Report von Datto mit den Aussagen von mehr als 1.400 MSPs bestätigt: Die Anzahl von Ransomware-Attacken gegen KMU steigt deutlich. 85 Prozent der MSPs berichten von Angriffen gegen KMU in den letzten zwei Jahren, 2018 waren das noch 79 Prozent.

Die Folgen eines Ransomware-Angriffs können verheerend sein. 64 Prozent der MSPs bestätigen einen Verlust der Unternehmensproduktivität ihrer KMU-Kunden nach einem erfolgreichen Angriff, 45 Prozent berichten von geschäftsbedrohenden Ausfallzeiten. Die Kosten für die Ausfallzeit der IT-Systeme betragen durchschnittlich 121.500 Euro, was einem Anstieg von mehr als 200 Prozent gegenüber den Angaben aus dem Vorjahr entspricht (2018: 40.500 EUR).

Lösungsansätze? 2-Faktor-Authentifizierung, BCDR-Lösungen und geschulte Mitarbeiter

Um die Wahrscheinlichkeit eines erfolgreichen Ransomware-Angriffs zu reduzieren, sollten MSPs die 2-Faktor-Authentifizierung (2FA) für jede Technologie einsetzen, die sie für ihre Kunden und für ihr eigenes Unternehmen nutzen. Auch wenn dies die einfachste und effektivste Maßnahme gegen Ransomware ist, wird sie nicht ausreichend genutzt. MSPs berichten, dass 2FA nur bei 60 Prozent der eMail-Clients und bei 61 Prozent der Passwort-Manager angewendet wird.

Business Continuity & Disaster Recovery (BCDR)-Lösungen bleiben laut MSPs weiterhin die effizienteste Maßnahme, um die Auswirkungen eines Ransomware-Angriffs zu begrenzen. 92 Prozent der befragten MSPs geben an, dass die Wahrscheinlichkeit, nach einem Ransomware-Angriff lange Ausfallzeiten zu haben, für Kunden mit BCDR-Lösungen sehr viel geringer ist.

Ein weiterer entscheidender Erfolgsfaktor für die Abwehr von Ransomware ist die konsequente Schulung der Mitarbeiter. 67 Prozent der befragten MSPs geben an, dass Phishing-Mails die Hauptursache für erfolgreiche Attacken sind. MSPs sollten ihre Position als IT-Berater nutzen, um KMU darüber aufzuklären, wie sie sich vor einem Ransomware-Angriff schützen können. Das schließt Maßnahmen zur Mitarbeiter-Schulung und die einzusetzenden Tools mit ein.

Den vollständigen Ransomware Report von Datto erhalten Sie kostenlos unter **www.datto.de**

ISO 27001 trifft Datenschutz – die neue ISO 27701

Spätestens mit der Anwendung der 2016 in Kraft getretenen EU-Datenschutz-Grundverordnung (DS-GVO) erhält der Schutz personenbezogener Daten eine Dimension, die bei betroffenen Unternehmen einen teilweise erheblichen Handlungsbedarf erfordern kann.

ISO 27001 und DS-GVO – Ein Vergleich

Mit Blick auf die DS-GVO kann ISO 27001, die internationale Norm für ein Informationssicherheits-Managementsystem (ISMS), Unternehmen, die personenbezogene Daten verarbeiten, gute Dienste leisten. Dies ist vor allem darin begründet, dass auch Datenschutz ein Thema innerhalb der Norm ist (ISO 27001, A.18.1.4 „Privatsphäre und Schutz von personenbezogener Information“). Mit der Erfüllung dieser Normanforderung werden gleichzeitig Bereiche der DS-GVO abgedeckt.

Das Delta

Der Anwendungsbereich eines ISMS kann nach ISO 27001 frei abgesteckt werden. Das bedeutet, dass der Umgang mit personenbezogenen Daten unter Umständen nicht oder nur zum Teil abgedeckt wird. Die DS-GVO enthält hingegen einige Anforderungen, die mit Blick auf ISO 27001 nicht relevant sind. Dazu gehört z. B. die Notwendigkeit, einen Datenschutzbeauftragten zu benennen. Auch muss sichergestellt sein, dass Betroffene Auskunft zu ihren Daten erhalten können und dem Recht auf Berichtigung ihrer Daten bzw. auf deren Löschung entsprochen wird.

ISO 27701 – Privacy Information Management System (PIMS)

Mit dem Ziel einer noch besseren Verknüpfung zwischen ISO 27001 und Datenschutz wurde im August 2019 die ISO 27701 veröffentlicht. Sie baut auf ISO 27001 auf und ergänzt diese um Datenschutzkriterien. Bei der Betrachtung des Kontextes der Organisation wird z. B. die Einbeziehung relevanter Datenschutzgesetze und gerichtlicher Entscheidungen verlangt. Ebenso sind bei der Risikobeurteilung Kriterien der Verarbeitung von personenbezogenen Daten zu berücksichtigen. Durch diese Erweiterung werden die Anforderungen an ein Datenschutz-Informations-Management-System (PIMS) in ein ISMS integriert.

Mit der DQS in mehr Informationssicherheit einsteigen

ISO 27701 ist allerdings keine Zertifizierungsnorm, die einem Verfahren im Sinne des Art. 42 DS-GVO entspricht. Als fachkundiger, akkreditierter Zertifizierer auditiert die DQS GmbH Ihr ISMS nach ISO 27001. Oder Sie lassen Ihren Datenschutz-Status mit Hilfe einer GAP-Analyse ermitteln – wir freuen uns auf das Gespräch mit Ihnen.

Ausgezeichnete IT-Sicherheit trifft auf sportliche Spitzenklasse

ESET, Ihr führender europäischer Sicherheitsanbieter, ist der neue Champion Partner von Borussia Dortmund.

eset IT SECURITY | BVB 09 Champion Partner

Mehr erfahren unter: www.eset.de

Im Bild v.l.n.r.: Holger Suhl (ESET Country Manager DACH), Carsten Cramer (Geschäftsführer Borussia Dortmund)

Gastbeitrag

Foto Westfalenpark: Roland Gorecki, Stadt Dortmund

Der Digital-Standort Dortmund

Dortmund hat seine montanindustrielle Vergangenheit hinter sich gelassen, in dieser Zeit aber schon den Grundstein als IT- und Digitalstandort gelegt. So entstand 1957 das erste Software-Systemhaus Europas in Dortmund! Seitdem hat sich Dortmund als Digitales Oberzentrum mit über 1.000 spezialisierten Software Unternehmen entwickelt.

Fakten zum DigitalStandort Dortmund:

- **Digitale Hochburg** zwischen Ruhrgebiet und Westfalen mit hartem B2B-Fokus
- Über **1.000 IT-Unternehmen** in Dortmund (Schwerpunkt Software)
- Knapp **17.000 Beschäftigte** in der IT-Branche (Anstieg von ca. 6,5% pro Jahr)
- **9.000 IT-Studierende** an den Hochschulen in Dortmund
- **Erste und größte IT-Fakultät Deutschlands** an der TU Dortmund
- **Größte IT-Fakultät der Fachhochschulen** in NRW an der FH Dortmund
- **Inkubatoren:** „B1st Software-Factory“, „e-Port“, „Digital HUB Logistics“
- **Angebote für Unternehmen:** u.a. Digitale Werkbank, Digitale Woche Dortmund
- **Forschung und Entwicklung:**

  Fraunhofer Institute – „ISST“ und „IML“,

  Europäisches Institut für Blockchain

  Forschungsinstitut für Telekommunikation und Kooperation,

  Kompetenzzentrum des Bundes für maschinelles Lernen (M2LR),

  Institut für die Digitalisierung von Arbeits- und Lebenswelten (IDiAL)

„So machen wir das“ – Ziele, Themen, Projekte und Gründungen

„Digitalisierung leistet einen wichtigen Beitrag für die wirtschaftliche und ökologische Zukunft unseres Landes. Digitalisierung hilft unserer Industrie, dem Handel und dem Handwerk sich den heutigen Anforderungen zügig anzupassen und dabei zukünftig auch im internationalen Vergleich stark zu bleiben. Daher haben wir uns von einer Industriemetropole zu einem Hotspot für digitale Lösungsanbieter mit industriellem Fokus entwickelt“, so Thomas Westphal, Geschäftsführer der Wirtschaftsförderung Dortmund.

Foto Herr Westphal: Wirtschaftsförderung Dortmund

THE PLACE TO BE.

CSF Cyber Security Fairevent

Dortmund, 04.–05. März 2020

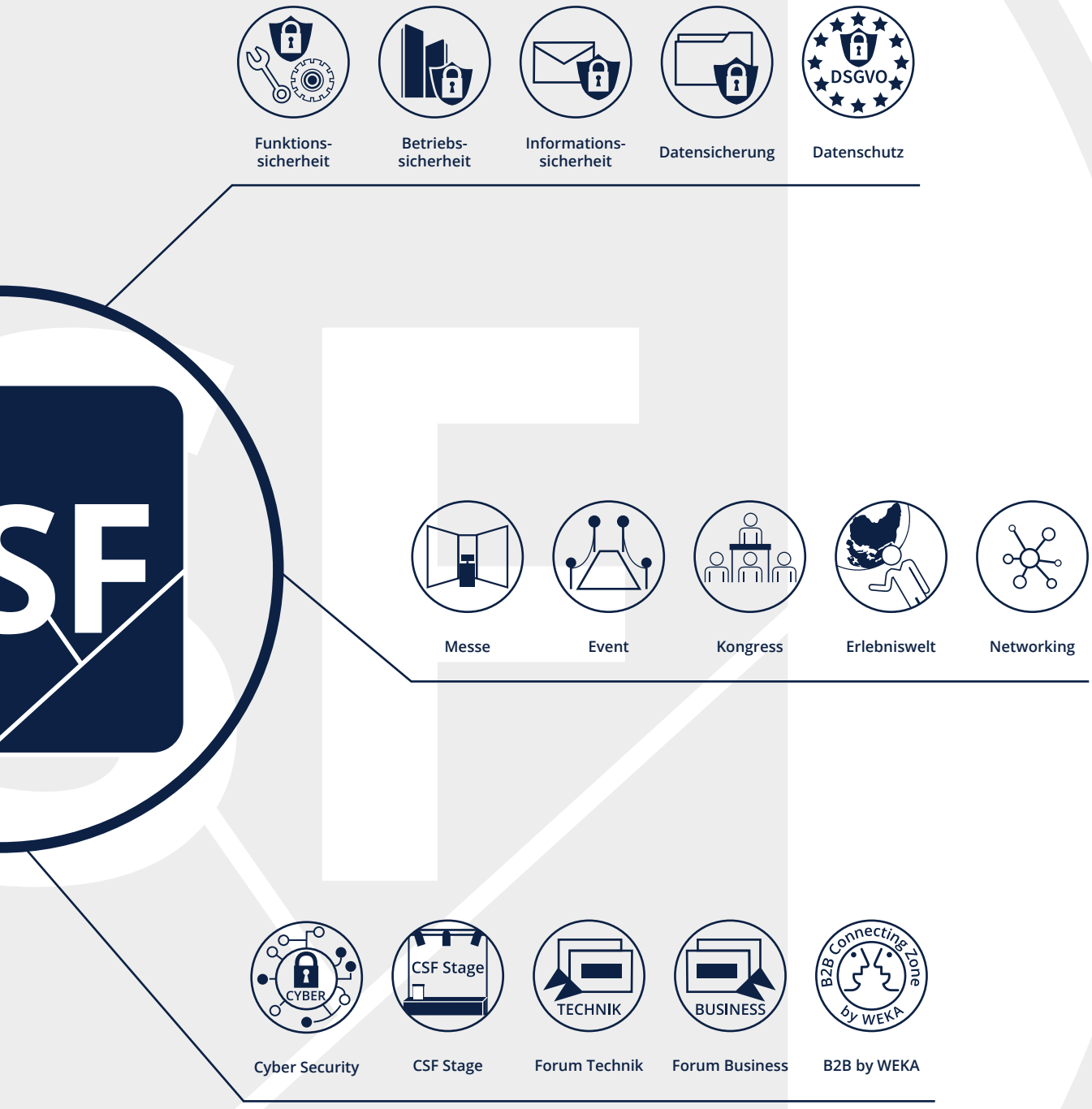
Überblick CSF

Cyber Security Fairevent

Show Act | Ruhezonen | Getränke | Kaffeebuffet | Bier & Brezen

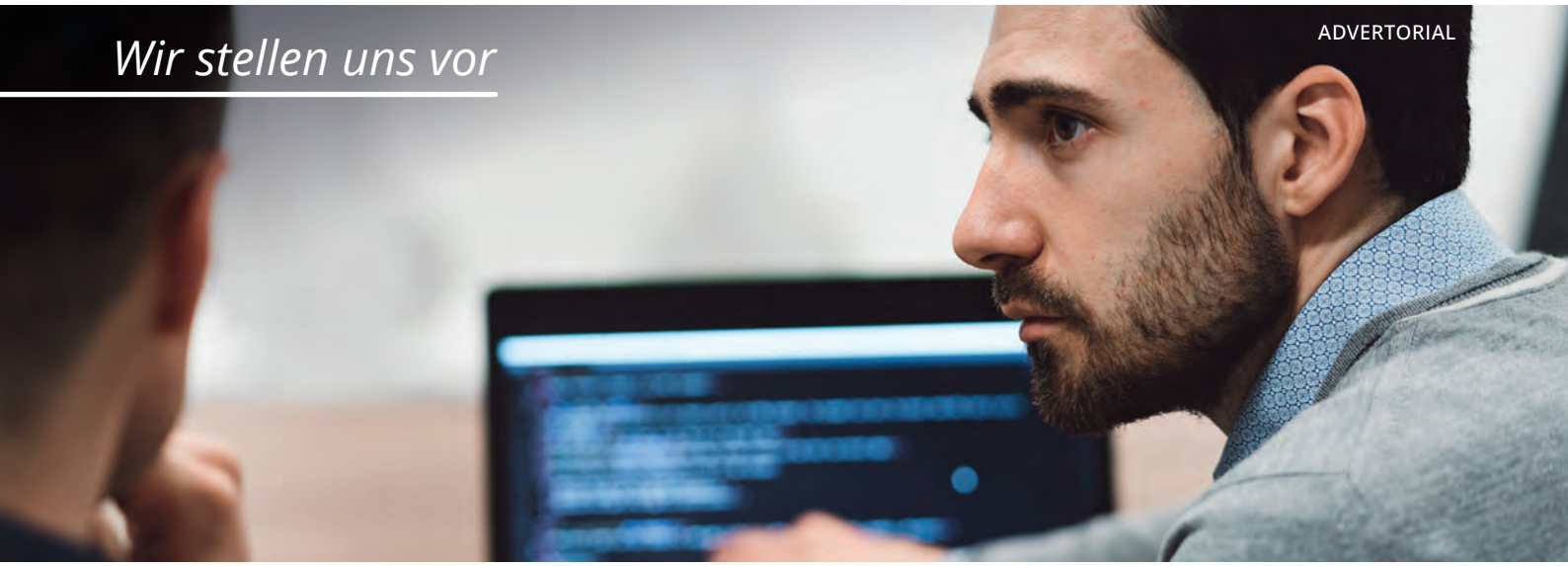
Erlebnisexponat Flipper | Erlebnisexponat Kicker | Erlebnisexponat Motorrad | Erlebnisexponat Boxen | Erlebnisexponat Escape Room

Keynote Speaker | Solution Panel | Moderatoren | Experten-vorträge | Live Hacking


Funktions-sicherheit
Betriebs-sicherheit
Informations-sicherheit
Datensicherung
DSGVO
Datenschutz
SF
Messe
Event
Kongress
Erlebniswelt
Networking
CYBER
Cyber Security
CSF Stage
CSF Stage
TECHNIK
Forum Technik
BUSINESS
Forum Business
B2B Connecting Zone by WEKA
B2B by WEKA

Wir stellen uns vor

ADVERTORIAL



Wie man gezielte Cyberattacken erkennt

IT-Sicherheitsspezialisten in Unternehmen stehen heute allerlei Abwehrmechanismen gegen Cyberattacken zur Verfügung. Zum Beispiel Firewalls, klassische Endpoint Protection oder auch Schwachstellenmanagement. Das wird gerne als Rundumschutz, der kaum Lücken für erfolgreiche Attacken lässt, gesehen. Leider gibt er Unternehmen aber ein falsches Gefühl von Sicherheit, wie die Realität zeigt.

Gezielte Attacken umgehen die präventiven Sicherheitsmaßnahmen und es dauert im Durchschnitt 69 Tage, bis ein Sicherheitsvorfall überhaupt entdeckt wird.

Fortschrittliche Angreifer wissen ganz genau, wie sie die präventiven Sicherheitsebenen umgehen und sich unbemerkt im Unternehmensnetzwerk bewegen können. Diese Attacken können nur durch eine Verhaltensanalyse erkannt werden. Hier bietet der Einsatz einer EDR-Lösung Möglichkeiten zur Erkennung und Reaktion auf fortschrittliche und gezielte Attacken.

Das Thema EDR stand lange Zeit nur bei sehr großen Unternehmen mit einem besonders ausgeprägten Sicherheitsbedürfnis auf der Agenda. Nun auch mehr und mehr bei kleinen und mittelständischen Unternehmen. Früher waren es die von Regierungen oder Behörden finanzierten Bedrohungsakteure, die anspruchsvolle und zielgerichtete Cyberattacken auf beispielsweise andere Nationen durchführen konnten. Jetzt aber stehen diese Techniken auch für durchschnittliche Cyberkriminelle zur Verfügung und geben ihnen nun die Möglichkeit, komplexe Angriffe auch gegen Unternehmen zu fahren. Die Angriffe werden zielgerichteter und anspruchsvoller. Die Abwehr dagegen hinkt meist hinterher. EDR-Lösungen sind leicht zu implementieren, haben eine hohe Verfügbarkeit und sind im Vergleich eines eigenen SoC deutlich günstiger. Während bei einem eigenen SoC mit In-House-Lösung das Know-How erst aufgebaut werden muss, „kauft“ sich das Unternehmen mit EDR eine Lösung, die von Beginn an aus einem Team hochqualifizierter Sicherheitsfachleuten besteht.

EDR-Lösungen bieten rund um die Uhr Dienste zur Bedrohungsüberwachung, Erkennung und Reaktion an und bieten Analysen um Bedrohungen wirksam zu bekämpfen. So setzen EDR-Lösungen Sensoren ein, um Metadaten von den Systemen eines Unternehmens zu erfassen. Die Metadaten werden z.B. kontinuierlich auf Anzeichen von Kompromittierungen durch Machine Learning analysiert. Zum Beispiel hat ein mittelgroßes Unternehmen mit etwa 650 Sensoren jeden Monat über eine Milliarde Alarme, aber nur etwa zehn von diesen Vorfällen müssen aktiv angegangen werden. Es braucht also immer noch die menschliche Expertise, wenn auch nicht mehr im vollen Maße.

F-Secure

F-Secure GmbH

Kistlerhofstr. 172c
81379 München
+49-89-787467-0

www.f-secure.com

Unternehmen sicher gegen Cyberangriffe machen

Ein unbedarfter Klick auf einen Link reicht aus, um im schlimmsten Fall die gesamte IT-Infrastruktur eines Unternehmens lahm zu legen oder wichtige Daten zu verlieren. Nicht umsonst sehen 87 Prozent der Unternehmen untrainierte Angestellte als größte Schwachstelle für Cyberattacken an, wie der Think-Tank ESI ThoughtLab herausfand. Mitarbeiter müssen daher ein Teil der Verteidigung werden und über das nötige Wissen verfügen, um IT-Security-Vorfälle zu verhindern. Die Lösung sind gezielte Schulungen: G DATA bietet mit seiner Cyber Defense Academy ein E-Learning-Portfolio mit Security Awareness Trainings an, was genau das leistet.

Mitarbeiter als Teil des IT-Security-Konzeptes sehen

Technische Maßnahmen, wie der Einsatz einer leistungsfähigen und umfassenden Sicherheitslösung, sind heute nur ein Baustein in der Strategie zum Schutz vor Cyberangriffen. Ein Konzept für einen umfänglichen Schutz muss weiter greifen und den „Faktor Mensch“ mit einschließen. Mit Hilfe der G DATA Security Awareness Trainings machen IT-Verantwortliche die Mitarbeiter im Unternehmen zu einem bedeutenden Teil der Abwehr und statten sie mit dem nötigen Fachwissen aus.

Die G DATA Security Awareness Trainings umfassen mehr als 30 Kurse zu verschiedenen Themen der IT-Sicherheit, die für den Arbeitsalltag wichtig sind - zum Beispiel Social Engineering, Arbeiten in der Cloud oder Phishing. Dabei wird das Wissen in Form von kurzen E-Learning-Einheiten praxisnah und nach den neuesten Lernmethoden bedarfsgerecht vermittelt. In den einzelnen Einheiten kommen sowohl Videos, als auch Texte zum Einsatz. So können Mitarbeiter diese einfach in ihren Arbeitsalltag integrieren. Die Lerninhalte verfestigen sich durch Wiederholungen und kurze Lernstandskontrollen.

Bedarfsgerechte Schulung

Bevor die Trainings starten, führen IT- und Personalverantwortliche einen kleinen Wissenstest bei den Mitarbeitern durch. So wird schnell klar, welche Lücken bestehen. Auf Grundlage dieser Ergebnisse lässt sich die Reihenfolge der Trainings festlegen und zunächst der dringendste Schulungsbedarf angehen. Nach und nach absolvieren die Angestellten alle Trainings, um ihr Wissen über IT-Sicherheit zu vervollständigen und alle Risiken beim Umgang mit den IT-Systemen zu kennen. Durch kontinuierliche Wiederholungen festigt und vertieft sich das Gelernte weiter. Diese Methodik versetzt Mitarbeiter in die Lage, richtig zu handeln und Bedrohungen im Keim zu ersticken.

G DATA CyberDefense AG

Königsallee 178
D-44799 Bochum
+49 (0) 234 / 97 62-0

Awareness Trainings

Gastbeitrag

Ruhiger Schlaf statt Cyber Angst

Es schon bedenklich, welche Mengen an schwarzmalerischen Szenarien einem zur Jahreswende auf den Desktop flattern. Die Anbieter von Cyber Security Software überschlagen sich förmlich mit Bedrohungsszenarien, vor denen Unternehmen stehen. Das Schlimme ist: Vieles davon dürfte durchaus zutreffen. Was Unternehmen und ihre Stakeholder aber statt Cyber Angst vor allem brauchen, ist Vertrauen in die Sicherheit der eingesetzten Abwehrsysteme.

So ist laut einem Bericht von Trend Micro zu erwarten, dass Firmen 2020 mit zunehmenden Risiken aufgrund ihrer Cloud-Infrastrukturen und digitalen Lieferketten zu kämpfen haben. Die wachsende Beliebtheit von Cloud- und DevOps-Umgebungen werde sie neuen Gefahren aussetzen, die aus der Angreifbarkeit von Drittanbietern resultieren. „Angreifer werden zunehmend versuchen, auf Unternehmensdaten in der Cloud zuzugreifen und dabei Deserialisierungs-Bugs, Cross-Site-Scripting und SQL-Injection nutzen“, ist Richard Werner, Business Consultant bei Trend Micro, überzeugt.

Auch die 5G Technologie wird sich fundamental auf die Cybersicherheit auswirken, glaubt Dan Schiappa, Chief Product Officer bei Sophos. Ja, 5G verspricht, fast alle Aspekte des Lebens mit atemberaubender Geschwindigkeit und geringerer Latenzzeit zu vernetzen. Aber, die Technologie wird auch erhebliche Sicherheitsrisiken mit neuen potenziellen Einstiegspunkten mit sich bringen und Unternehmen neuen Angriffstypen aussetzen. „Während die Funktechnologie ein enormes Potenzial bietet, öffnet sie gleichzeitig die Büchse der Pandora. Geräte mit 5G-Technologie werden keine direkte Vernetzung mit dem Firmennetzwerk mehr erfordern. Dies macht es unglaublich schwierig, Bedrohungen und gefährdete Geräte zu identifizieren“, prophezeit der Experte.

Damit nicht genug, droht eine weitere Höllenmaschine am Horizont. „Der Impact des Quantencomputers auf die IT-Sicherheit wird einem Erdbeben gleichen“ warnt Frank Balow, Kryptografie-Spezialist und Director Consulting Identity and Key Management, CISSP bei der Security Division von NTT. Unternehmen sollten daher versuchen, die möglichen Auswirkungen auf die gesamte Infrastruktur, aber auch auf einzelne Passwörter, Applikationen, Systeme und Datenrechtzeitig zu antizipieren.

Vor dem Hintergrund derartiger Szenarien brauchen Unternehmen mehr denn je Vertrauen in die Sicherheit der eingesetzten Abwehrmaßnahmen. In diese Richtung zielen etwa die Cybersecurity-Zertifikate für Produkte, Prozesse und Dienstleistungen, die die EU im vergangenen Juni auf den Weg gebracht hat. Bis diese in der Lage sind, Vertrauen herzustellen, dauert es noch: Eine Liste verbindlicher Zertifizierungsschemata vorzulegen, plant die Europäische Kommission erst bis zum 31.12.2023. Eine schnellere Lösung könnten dagegen womöglich „Trust Based Services“ liefern. Analog zum Testat finanzieller Kennzahlen, dass Wirtschaftsprüfer ihren Mandanten jedes Jahr verleihen, könnten sie auch die Sicherheit der eingesetzten Abwehrmaßnahmen bestätigen und Unternehmens-Chefs und Anteilseigner ruhiger schlafen lassen.

Heiner Sieger

Chefredakteur
DIGITAL BUSINESS
CLOUD
www.win-verlag.de

indevis – Sicherheit in einer vernetzten Welt

Die indevis GmbH ist Ihr verlässlicher Partner in Sachen IT-Sicherheits-, Datacenter- und Netzwerklösungen. In diesen Bereichen unterstützen wir seit über 20 Jahren Unternehmen jeder Größe und Branche mit unseren Managed Security Services, die wir als Cloud- und on-premises-Lösung anbieten.

Cloud based und on-premises based Managed Security Services

Bei unseren cloud-basierten Managed Security Services werden bestimmte IT-Sicherheits- und Netzwerkdienste aus den indevis Rechenzentren erbracht, bzw. dorthin ausgelagert und von zertifizierten Spezialisten kompetent betreut. Mit der on-premises based Variante besteht die Möglichkeit, die Sicherheitstechnologie inhouse im eigenen Rechenzentrum zu betreiben, wobei indevis Installation und Betriebsverantwortung übernimmt.

So können wir allen Unternehmen je nach Anforderungen und Bedürfnissen eine zuverlässige, entlastende und kosteneffiziente Alternative zum aufwendigen, eigenverantworteten Inhouse-Betrieb von IT-Sicherheits- und Netzwerklösungen zur Verfügung stellen. Durch professionelle Management- und Supportdienste wird dies abgesichert.

Neben unseren Managed Security Services bieten wir außerdem innovative und marktführende Herstellerlösungen an, die unsere Kunden vor Bedrohungen aller Art aus dem Internet schützen und die Verfügbarkeit der IT-Systeme sicherstellen. Wir decken mit unseren Lösungen das gesamte Spektrum von Endpoint-, über Netzwerk- bis Cloud-Security ab.

Zertifizierung nach ISO 27001

indevis erfüllt sowohl die Anforderungen der Wirtschaft als auch die öffentlicher Behörden und Hochschulen. So unterliegen unsere Rechenzentren deutschen Datenschutzrichtlinien und erfüllen höchste Ansprüche in Bezug auf Ausfallsicherheit und Überwachung.

Da wir besonders praxisorientiert mit dem Thema IT-Sicherheit umgehen, haben wir uns für eine Zertifizierung nach der internationalen Norm ISO/IEC 27001 durch den TÜV Süd entschieden. Der Geltungsbereich der Zertifizierung umfasst das Managed Security Service Providing (MSSP) der indevis, alle für die angebotenen Services erforderlichen IT-Systeme und Prozesse, sowie die genutzten Rechenzentren.

indevis
Sicherheit in einer vernetzten Welt

indevis GmbH
Irschenhauser Straße 10
81379 München
Tel. +49 (89) 45 24 24-100

www.indevis.de

ADVERTORIAL

Wir stellen uns vor

Angriffe abwehren und Bedrohungen erkennen mit Ixia ThreatARMOR

Kein Netzwerk und kein Server ist ohne den Einsatz von diversen Security Tools, wie Firewall, IPS, Antivirus, DLP und (normalerweise) einem SIEM-System, mit dem Internet verbunden. Und obwohl Hacker beim Eindringen in Netzwerke und Ausspähen von Daten Spuren hinterlassen, sind neue Schlagzeilen über große und eigentlich vermeidbare Angriffe an der Tagesordnung.

Warum also können nicht mehr Angriffe verhindert werden? Der Grund: Alert Fatigue. SecOps Teams arbeiten unermüdlich, um Angriffe zu verhindern, aber die schiere Menge an Warnmeldungen ist erdrückend.

Die ständige Flut an Warnungen von Security Tools machen es selbst für die wachsamsten Security Teams unmöglich, die relevanten Spuren eines Angriffs oder Datendiebstahls rechtzeitig zu finden.

Verkleinern Sie Ihre Angriffsfläche mit ThreatARMOR

ThreatARMOR verkleinert Ihre Angriffsfläche mit einen ständig aktuell gehaltenen Filter für den ein- und ausgehenden Datenverkehr Ihres Netzwerks und eliminiert so Trafic mit und von bereits bekannten bösartigen Absendern und aus nicht vertrauenswürdigen Ländern.

Sie denken jetzt vielleicht: „Meine Firewall macht das doch bereits“. Ein grundlegendes Problem heutiger Cyberattacken ist aber, dass diese von kurzlebigen IP-Adressen ausgehen. Um der Aufdeckung zu entgehen, werden IP-Adressbereiche dabei ständig gewechselt.

Sie müssen also Angreifer daran hindern, Ihr Netzwerk überhaupt zu erreichen — und hier spielt ThreatARMOR seine Stärken aus. Durch das Blocken von Phishing- und Malware-Seiten, Botnetz-Controllern, kompromittierten Netzwerken und nicht zugewiesenen IP-Adressbereichen schafft es ***ThreatARMOR, die Anzahl bösartiger und ungültiger Pakete, durch die Warnmeldungen ausgelöst werden, um 80 % zu reduzieren***. Das reduziert die Alert Fatigue und Ihre Experten können sich nun ganz darauf konzentrieren, ihre eigentlichen Aufgaben zu erfüllen anstatt irrelevanten Warnmeldungen nachzugehen.

Setzen Sie auf die führende Threat Intelligence der Branche

Durch den Einsatz Cloud-basierter Security-Validierung und exzellenter Skalierbarkeit, ThreatARMOR verwendet keine Signaturen, gehören False Positives der Vergangenheit an. Adressbereiche werden nur dann geblockt, wenn eindeutig feststeht, dass von diesen IPs kriminelle Aktivitäten ausgehen, wie beispielsweise die Verteilung von Malware oder Phishing. Belegt wird dies durch das Datum der letzten bekannten Aktivität und Screenshots.

Als weltweiter Marktführer bei Application- und Security-Tests hält Ixia im Application und Threat Intelligence (ATI) Research Center den Bedrohungs-Feed ständig Up-2date, indem jeder Datensatz und geblockte Adressbereich täglich individuell geprüft und ThreatARMOR im Fünf-Minuten-Takt aktualisiert wird.

Netzwerkverfügbarkeit ist von größter Bedeutung für Ihr Unternehmen und ThreatARMOR wurde speziell unter diesem Aspekt entwickelt. Features wie doppelt redundante Netzteile und ein Ethernet Interfaces mit integriertem Bypass Mode garantieren maximale Stabilität und Ausfallsicherheit sowohl bei den 1 GbE Kupfer- als auch den 10 GbE Glasfaser-Interfaces

Bauen Sie Ihre Verteidigung mit Ixia aus

Angreifer gehen geschickt vor. Wenn Sie nicht ständig einen Schritt voraus sind, fallen Sie zurück. Besuchen Sie *www.ixiacom.com/threatarmor* um zu erfahren, wie Sie die Sicherheit in Ihrem Netzwerk mit ThreatARMOR ausbauen können.

ixia
A Keysight Business

Ixia Solutions Group,
Keysight Technologies Deutschland

Herrenberger Str. 130 | 71034 Böblingen
Phone +49 7031 4641

www.ixiacom.com

SECURING CYBERSPACE.

CSF Cyber Security Fairevent

Gastbeitrag

Cyber Security als Geschäftstreiber bei Versicherern

Cyber Security muss als Business Enabler gesehen werden, nicht als Kostentreiber. Was sind die Top-Themen der Cyber Security in den nächsten Monaten? Klar ist: Wir gehen einem Zeitalter signifikanter Datenverletzungen entgegen. Konsequenz: Dem Top-Management in der Versicherungswirtschaft kommt mehr denn je eine Schlüsselrolle zu. Cyber Security sollte deshalb als Teil des Business Cases betrachtet werden und nicht als reiner Kostentreiber. Cyber Security ist idealerweise sowohl Risiko-Beratung als auch Business Enabler.

1. Die Wucht der Attacken steigert sich: Weitere Angriffswellen werden folgen, neu ist die Wucht, mit der die Attacken geführt werden. Das wirft die zentrale Frage auf, wie sicher die vernetzen Geräte, die IT-Netzwerke und die Infrastrukturen sind. Wer trägt die Verantwortung, wenn Cyber-Security-Maßnahmen nicht ausreichen? Müssen Auflagen und Kontrollen weiter verschärft werden?

2. Das Internet der Dinge erfordert verbindliche Sicherheitsstandards: Smarte Geräte werden immer beliebter, umso dringender wird der Schutz der Privatsphäre. Eher früher als später werden Hersteller vernetzter Geräte höhere Sicherheitsstandards einführen müssen. Freiwillige oder verpflichtende Cyber-Security-Prüfungen und Zertifizierungen für vernetzte IoT-Geräte (IoT = Internet of Things, Internet der Dinge) vor der Markteinführung werden wahrscheinlicher.

3. 2020 wird das Jahr der Cloud-Security-Lösungen: Die Sensibilität dafür, dass beim Einsatz von Cloud Services das IT-Netzwerk noch besser abgesichert werden muss, steigt. Sicherheitslösungen, die den Netzwerkverkehr zwischen dem Cloud-nutzenden Unternehmen und dem Cloud Service Provider überwachen, werden verstärkt nachgefragt. Außerdem ist die Cloud selbst immer häufiger Quelle für den Abruf von Sicherheitslösungen, darunter Echtzeit-Sicherheitsanalysen und die Detektion von Anomalien durch Künstliche Intelligenz (maschinelles Lernen), aber auch Managed Services für Security Data Analytics, Continuous Monitoring und Incident Response Advisory Services.

4. IAM und die Cloud im Verbund
IAM (Identity- und Access-Management) und Cloud werden zur neuen äußeren Verteidigungslinie der Organisation. Cloud-Strategien werden stärker mit dem Bereich Rechte-, Zugriffs- und Passwort-Management verzahnt. Das Ergebnis sind eine konsistente Verwaltung von Benutzern und Berechtigungen über Rollen und eine sichere und benutzerfreundliche Authentisierung.

5. Nicht ohne Managed Security Services: Viele Unternehmen stehen der Auslagerung von Cyber Security an externe Partner nach wie vor kritisch gegenüber. Angesichts des anhaltenden Fachkräftemangels wird Vertrauen zu einem kompetenten externen Partner für Cyber Security zu einem der wichtigsten Erfolgsfaktoren für die Absicherung des Unternehmens, nicht zuletzt auch wegen der wachsenden Zahl an Innentätern.

Herbert Sebald

Chefredakteur
vb Versicherungsbetriebe
versicherungsbetriebe.de

Bring on securing your space

Die Technologien von heute eröffnen den Menschen bislang ungeahnte Möglichkeiten. Kaspersky sichert diese Technologien damit jeder Mensch jederzeit auf dem Weg in diese neue Zukunft geschützt ist. Digitale Sicherheit für das Leben von morgen.

kaspersky

BRING ON THE FUTURE

Die weltweit verbreitetste Datenschutzmanagement-Software

ZUR GEWÄHRLEISTUNG VON DATENSCHUTZ-, SICHERHEITS- UND DRITTANBIETER-COMPLIANCE

Der schnelle Weg zur Compliance mit DSGVO, BDSG-neu, CCPA, ISO und über 100 weltweite Datenschutz- und Sicherheitsbestimmungen

Technologie zur Unterstützung im Bereich Datenschutz, Sicherheit und Risikomanagement von Drittparteien

Datenschutzmanagement	Datenschutz für Marketing und UX-Design	Risikomanagement von Drittparteien	Vorfallreaktion
Reifegrad und Planung Bewertung der Compliance-Berichte	**Cookie-Compliance** Website-Scanning und Cookie-Einwilligung	**Lieferantenbewertungen** Sicherheits- und Datenschutzrisiken	**Vorfallreaktion** Bewertungen, Benachrichtigungen und Berichte bei Datenpannen
Benchmarking Markt- und Unternehmensvergleich	**Compliance für mobile Anwendungen** App-Scanning und mobiles Einwilligungsmanagement	**Vendorpedia Risk Exchange** Sicherheits- und Datenschutzrisiken	**Aufnahme von Vorfällen** Zentrales Register
Bewertungsautomatisierung DSFA, TOMs, PbD und InfoSec	**Präferenzmanagement** Präferenz-Center für Endnutzer	**Vendorpedia Monitoring** Datenschutz- und Sicherheitsbedrohungen	**Risikobewertungen** Risiko- und Schadensanalyse
Verarbeitungsverzeichnis Inventar von Verarbeitungstätigkeiten und IT-Systemen	**Betroffenenanfragen und Verbraucherrechte** Ganzheitliches Management und Automatisierung	**Vendor Chasing Services** Zurückverfolgungs- und Validierungsdienst	**Benachrichtigung und Berichte** Verfolgung von Pflichten
Targeted Data Discovery Lokalisierung und Löschung betroffener Daten	**Richtlinien und Hinweise** Zentral hosten, verfolgen, aktualisieren	**Datenflüsse hinsichtlich Lieferanten** Automatisierte Berichte und Verzeichnisführung	**Echtzeit-Aktivitätsfeed** Datenpannen und Strafmaßnahmen

Definieren Sie gemeinsam mit uns eine neue Generation von Lösungen im Bereich Datenschutz, Sicherheit und Drittparteienrisiko

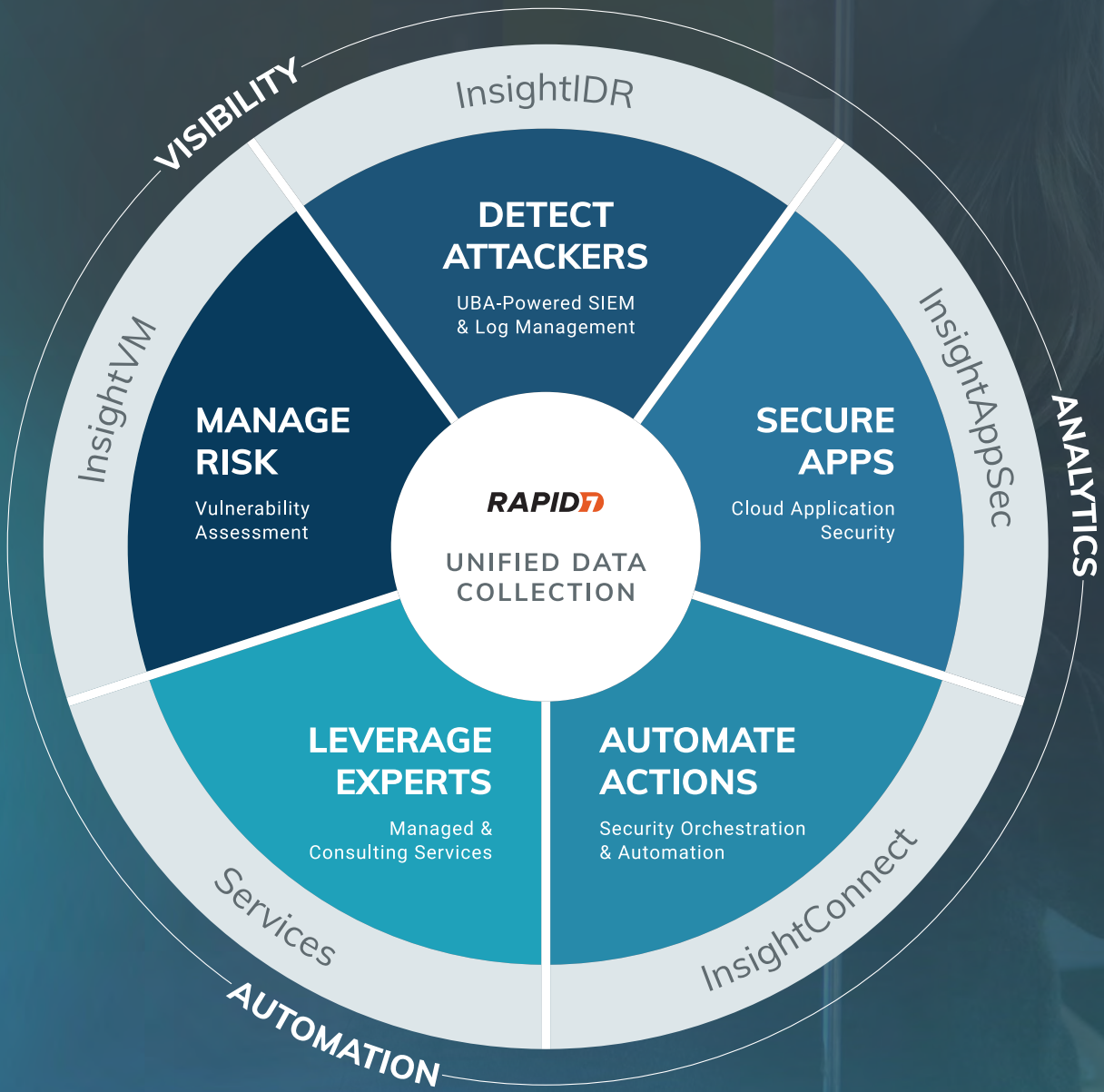
Leistungsstarke Technologieplattform	Regulatorische Forschung auf höchstem internationalem Niveau	Weltweiter professioneller Kundendienst	Eine große aktive Benutzer-Community
Unübertroffene Breite und Tiefe an Anwendungsfällen in den Bereichen Datenschutz und Sicherheit	**Die intelligenteste Plattform der Branche mit umfangreichen Regulierungsdatensätzen, die täglich aktualisiert werden**	**Die meisten weltweit verfügbaren zertifizierten Ressourcen zur Unterstützung Ihrer Implementierung**	**Die größte und aktivste globale Community zum Austausch von Best Practices**
Über 50 erteilte Patente	**40** interne Datenschutzforscher	**200** Implementierungsmitarbeiter	**Über 10.000** Teilnehmer
Über 60 Sprachen	**500** Anwälte im Netzwerk	**2.500** zertifizierte Partner	**Über 250** global Workshops
Über 300 Plug-ins	**300** abgedeckte Rechtsprechungen	**95%** Kundenzufriedenheit	**Über 100** Orte weltweit

OneTrust Privacy
PRIVACY MANAGEMENT SOFTWARE

RAPID7

Secure Advancement Happens Here.

Break down barriers. Innovate with confidence. See how with Rapid7.



TO LEARN MORE:

Visit us at **www.rapid7.com**.

Quantencomputer und die IT-Sicherheit

Quantencomputer sind die Zukunft. Was bedeutet das für die IT-Security?

Um mehr Leistung in Computer packen zu können, müssen dessen Teile immer kleiner werden. In naher Zukunft erreichen wir Maßstäbe, die sich unter der Größe von Atomen befinden – und wo ganz andere Regeln gelten: Dort verlassen wir nämlich das Reich der klassischen Physik und betreten die Sphäre der Quantenphysik. Computer, die in diesem Maßstab gebaut werden, unterscheiden sich fundamental. Sie basieren nicht mehr auf festen Ergebnissen, die entweder klar 0 oder klar 1 sind, sondern auf Wahrscheinlichkeiten. Wo ein klassischer Computer auf Bits setzt, die entweder 0 oder 1 sind, basiert ein Quantencomputer auf Quanten-Bits, kurz Qubits genannt. Diese unterscheiden sich dadurch, dass sie sowohl einen Wert 0 oder 1 einnehmen können als auch einen Wert dazwischen – mehr dazu später. Qubits sind jedenfalls die Eingaben für die Schaltungen der Quantencomputer, auf ihnen rechnet das System. Die Schaltungen selbst werden Quantengatter genannt.

Technologietrend Quantencomputer: In den letzten Jahren hat sich einiges getan auf dem Gebiet. Die Hauptakteure 2019 sind die USA und China, wobei die EU nachzieht. Präsident Trump unterzeichnete im Dezember 2018 den National Quantum Initiative Act, dessen Plan es ist, die Technologie in den nächsten 10 Jahren in den USA maßgeblich voranzutreiben. Google veröffentlichte 2018 einen 72-QuBit-Rechner namens Bristlecone, und IBM bietet über "Q Experience" nunmehr direkten Zugriff auf Quantencomputer via Cloud für jedermann. Der zuletzt herausgebrachte „IBM Q System One" ist erstmals ein Quantencomputer, der speziell für den wirtschaftlichen Einsatz gedacht ist. Die EU stellte 2018 ihrerseits 9,1 Millionen Euro für die Forschung zum Thema bereit. Gartner, ein Anbieter für Marktforschung, listet Quantum Computing als eines der Top 10 strategischen Technologietrends für 2019.

Was bedeuten Quantencomputer für die IT-Sicherheit? Mit Quantencomputern könnten bestimmte IT-Probleme künftig wesentlich effizienter gelöst werden als mit klassischen Rechnern. Das betrifft große Simulationen, Optimierungs- und Klassifizierungsprobleme ebenso wie Algorithmen für große Datenmengen sowie insbesondere Kryptographie und Kryptoanalyse. Kryptographie hat die Aufgabe, Informationen verschlüsselt zu übertragen und nach Empfang wieder zu entschlüsseln. Die Kryptoanalyse ist gegenteilig ausgelegt: Ihr geht es um das Brechen von Verschlüsselungen, ohne das dies von Sender und Empfänger gewollt bzw. bemerkt wird. Derzeit basiert die Kryptographie im Wesentlichen auf der Grundlage, dass gewisse mathematische Probleme nicht leicht zu lösen sind – und sich Angriffe schon wegen des hohen Rechenaufwands nicht lohnen. Mit Quantencomputern hingegen können viele mathematische Probleme in so kurzer Zeit gelöst werden, dass die zeitgenössische Kryptographie allein nicht mehr ausreicht.

Der Quantencomputer als Rechengenie: Wo ein herkömmlicher Rechner entweder Nullen oder Einsen zur Verfügung hat, um Dinge zu berechnen, hat ein Quantencomputer die 0 und die 1 gleichzeitig zur Verfügung. Das heißt, er kann parallel auf beiden Zuständen rechnen. Oder anders ausgedrückt: Ein Algorithmus rechnet sowohl das Ergebnis für 0 als auch das Ergebnis für 1 in einem Schritt aus.

- Bei 2 Bits sind das vier Zustände, auf denen parallel gerechnet wird: 00,01,10 und 11.
- Bei 3 Bits sind es dann schon 8 Zustände: 000, 001, 010, 011, 100, 101, 110 und 111.
- Insgesamt ergibt sich so ein exponentielles Wachstum des Berechnungsraums von 2x, mit x der Anzahl der Qubits.

Beispiel RSA: Um das Problem besser zu verstehen, schauen wir uns an, wie eines der großen Kryptographieverfahren im Kern funktioniert: RSA. Dieses findet man heutzutage in vielen Anwendungsbereichen, etwa bei der Verschlüsselung des Internets, von Telefonen, E-Mails oder im Electronic Banking. RSA basiert auf der Schwierigkeit, eine Zahl, die aus einer Multiplikation entstanden ist, wieder in die ursprünglichen 2 Zahlen zu zerlegen. Diese ursprünglichen 2 Zahlen sind speziell: man kann sie nur durch sich selbst oder durch 1 teilen – es handelt sich also um Primzahlen. Der auf den ersten Blick naheliegende Weg, a und b zu finden, wäre es, alle Multiplikationen durchzuprobieren, bis am Ende c gefunden ist. Was mit steigender Größe der Zahlen immer komplizierter werden dürfte, da die Komplexität aufgrund der Menge möglicher Primzahlen sehr schnell zunimmt. Selbst die schnellsten bekannten

Algorithmen für klassische Computer können das Problem ab einer bestimmten Zahlengröße nicht mehr lösen.

Der Shor-Algorithmus für Quantencomputer: Anders Quantencomputer. Für diese gibt es einen Algorithmus, der die Lösung in wesentlich kürzerer Zeit liefern kann: der Shor-Algorithmus. Dieser wurde 2001 erstmals experimentell für die Zahl 15 durchgeführt, die damit erfolgreich in die Zahlen 3*5 zerlegt wurde. Das nachfolgende Bild zeigt grob skizziert, wie man sich den Unterschied zwischen klassischem und Quantencomputer vorstellen kann. Dabei unterscheidet man den exponentiellen Aufwand vom polynomiellen. Klassische Computer benötigen exponentiell viel Aufwand für die Primfaktorzerlegung, Quantencomputer polynomiell viel. In der Darstellung werden 2 Funktionen aus diesen beiden Klassen gezeigt: 2x und x^2. In der Realität sind die Funktionen für den Aufwand in beiden Algorithmen komplexer aufgebaut. Die hier gewählten einfacheren Funktionen sollen zur Veranschaulichung des Unterschieds dienen. Der Shor-Algorithmus kann aber noch mehr. Er bricht neben RSA auch andere gängige Kryptographieverfahren:

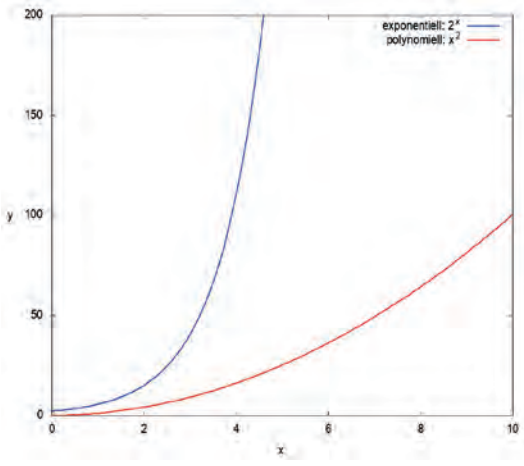


Bild 1: Verlaufskurve Shor Algorithmus.

Elliptische Kurven und diskrete Logarithmen. (Bild 1) Für RSA benötigt er eine Mindestanzahl von Qubits: 2n+3, wobei n die Anzahl der Bits derjenigen Zahl ist, die zu faktorisieren ist. Das heißt: Wurde RSA mit einer Zahl versehen, die mit 1024 Bits dargestellt werden kann, so benötigt der Shor-Algorithmus mindestens 2*1024+3 = 2050 Qubits, um diese Zahl effizient zu zerlegen.

Auch die Kryptographie entwickelt sich weiter: Zum Glück hat sich auch die Kryptographie weiterentwickelt, weil das Problem frühzeitig erkannt und beforscht wurde. Aus dieser Forschung sind kryptographische Methoden hervorgegangen, die auch Quantencomputern standhalten können. Diese Form der Kryptographie wird Post-Quantum-Kryptographie genannt. Zum Teil sind ihre Methoden schon heute in gängigen Kommunikationstools wie SSH vorgesehen.

Experimente mit Quantencomputern: Wer Lust hat, mal ein bisschen mit Quantencomputern herumzuspielen, kann sich einen Account bei IBM anlegen und direkt auf einem Quantencomputer Schaltungen erzeugen, die dann über die Cloud auf IBM Q Experience gesendet werden können. Zudem gibt es eine Menge aufkommender Programmiersprachen, die Quantencomputer simulieren können und mittelfristig für dessen Programmierung gedacht sind. Beispiele hierfür sind Microsoft Q#, Project Q und Qiskit für Python oder Circ. Hier ein paar Ideen zum Einsteigen: Man könnte zum Beispiel mit einem leeren System anfangen, das komplett mit Nullen initialisiert ist und einfach gemessen wird (Bild 2).

... Oder einfach mal ein Qubit negieren (Bild 3).

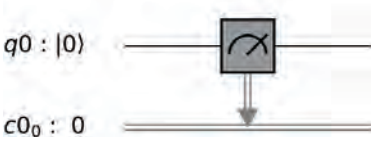


Bild 2: Messung eines Qubits (q0) und Übertragung des Ergebnisses auf ein klassisches Bit (c0).

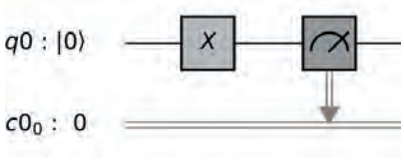


Bild 3: Qubits werden mittels eines Pauli-X-Gatters negiert.

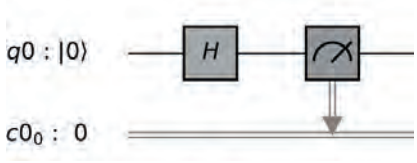


Bild 4: Hadamard-Gatter, um auf Qubits gleichzeitig 0 und 1 zu rechnen.

Der wichtigste, aber auch schwierigste Schritt ist, zu verstehen, wie man das System in den Modus versetzt, dass auf allen Qubits gleichzeitig gearbeitet wird. Hierfür ist das Hadamard-Gatter der erste Anlaufpunkt (Bild 4).

Grundsätzlich müssen wir Softwareentwickler uns darauf einstellen, dass die Dinge hier ein wenig anders laufen, als wir es gewohnt sind. Wichtig ist, dass wir uns davon nicht abschrecken und der Sache offen gegenüberstehen. Einen übersichtlichen, praktischen Einstieg mit Links bietet zum Beispiel diese Awesome List auf Github. Insgesamt bleibt die Entwicklung von Quantencomputern ein Thema, das derzeit in Forschung und Wirtschaft stark bearbeitet wird. Wir werden sehen, was die Zukunft bringt. Es dürfte spannend bleiben.

Matthias Altmann

Matthias Altmann ist IT-Security-Experte bei Micromata.

Quelle: it security 20-2019, S. 60ff

XG FIREWALL

Das Aus für unbekannte Bedrohungen.

- **Synchronized App Control**
erkennt automatisch unbekannte Anwendungen

- **Sandboxing mit Machine Learning,**
ATP, Dual AV, Web & App Control und Anti-Phishing

- **Automatische Reaktion auf Vorfälle**
durch Einsatz von **Synchronized Security**

www.sophos.de/xgfirewall

Platin-Award „Enterprise Network Firewalls" von SecurityInsider

Platin-Award „Identität und Sicherheit" von eGovernment Computing

Sophos XG Firewall – Beste Firewall im Test der unabhängigen NSS Labs

ITK-Produkte des Jahres im Bereich „Cybersecurity" von der Funkschau

„Hersteller des Jahres Security" von dem Channel-Fachmagazin CRN

SOPHOS

Die Evolution der Cybersecurity.

HUMBOLDT von Telonic sorgt für Sicherheit in Netzwerken

Industrie oder Verwaltung: Ohne Datennetzwerke sind Unternehmen und Institutionen nicht arbeitsfähig. Seit 1979 dreht sich die Arbeit des Kölner Systemhauses Telonic rund um Datennetzwerke und deren Sicherheit. Das über 100 Mann starke Expertenteam agiert herstellerunabhängig und liefert Kunden die jeweils ideale Sicherheits- und WAN-, LAN- oder WLAN-Lösung. Im Vordergrund stehen dabei Qualität, Ausfallsicherheit, einfaches Management und Zukunftssicherheit der Installationen. Ein eigenes Security Network Operation Center SNOC betreut Kunden und ihre Netzwerke 24 Stunden am Tag, sieben Tage in der Woche und 52 Wochen im Jahr zum Schutz vor Störungen und Bedrohungen.

HUMBOLDT analysiert Logdateien

In Netzwerken fallen täglich zahlreiche Log-Dateien an. Die Mehrzahl ist dabei harmlos und bedarf keiner Handlungen – wirklich ernste Meldungen werden jedoch in der Datenflut leicht übersehen. Dieses unnötige Risiko schließt HUMBOLDT als eigener Service von Telonic aus. HUMBOLDT analysiert mit Hilfe künstlicher Intelligenz sämtliche anfallenden Logdateien einer Security-Infrastruktur und gibt gezielte Handlungsanweisungen. Die unüberschaubare Anzahl von sicherheitsrelevanten Log-Einträgen aus unterschiedlichen Quellen wird von HUMBOLDT korreliert, bewertet und mit Aktionen versehen. Diese können vom Unternehmen selber oder durch Mitarbeiter von Telonic direkt vorgenommen werden. Neue Alarme ohne spezifische Handlungsanweisung werden durch das Telonic Computer Emergency Response Team (T-CERT) ausgewertet und mit einer Handlungsanweisung in HUMBOLDT versehen. Ab sofort werden diese Problemstellungen ebenso automatisiert bearbeitet. So entwickelt sich HUMBOLDT kontinuierlich weiter und wird zu einer umfassenden Wissensdatenbank. Der enorme Zeitaufwand für Security-Experten, um Schritte für eine Alarmnachverfolgung zu definieren, entfällt und wird durch direkte Anweisungen mit höchstmöglicher Genauigkeit ersetzt.

ISO-zertifizierter Service

Mit dem eigenen LifeLine-Service bietet Telonic rund um die Uhr die nötige Sicherheit, dass eine komplexe IT-Infrastruktur korrekt arbeitet. Mit einer speziell dazu entwickelten Technologie, dem IPrunner, überwacht das Team die Funktion eines Netzwerkes proaktiv. Damit haben Netzwerkbetreiber rund um die Uhr die nötige Sicherheit einer korrekt arbeitenden Infrastruktur.

Das Informations-Sicherheits-Management-System der Telonic ist gemäß ISO/IEC 27001 zertifiziert.

TELONIC
nonstop networking

Telonic GmbH
Albin-Köbis-Str. 2, 51147 Köln
Tel.: +49 2203 9648 0
Mail: kontakt@telonic.de

www.telonic.de

TUXGUARD

Cyber Security in Perfektion

ICH SEHE WAS,
WAS DU NICHT SIEHST

Modernste TUXGUARD-Technologien machen Gefahren aus dem Cyberraum sofort sichtbar. Mit dem TUXGUARD Management Center schützen und verwalten Sie Ihre Daten sicher in Echtzeit. Das ist Cyber Security in Perfektion.

TUX ENDPOINT TUX MAIL TUX FIREWALL

MADE IN GERMANY

www.tuxguard.com

Your Data.

Our Mission.

Is Your Data Safe?

At Varonis, protecting your file and email systems from cyberattacks and insider threats is our primary focus. We're fighting a different battle – so your data is protected first. Not Last.

Learn more at **www.varonis.com**

VARONIS

WatchGuard DNSWatchGo

Einfache Sicherheit für unterwegs.

DNSWatchGo von WatchGuard schützt Sie auch vor Cyber-Angriffen außerhalb der Firewall. Dieser Cloud-basierte Dienst bietet leistungsstarke Content-Filterung und mehr Sensibilisierung der Mitarbeiter durch aufschlussreiche Meldungen über erkannte Cyber-Risiken. Im Falle einer ernsthaften Bedrohung führen die Sicherheitsexperten von WatchGuard eine maßgeschneiderte Analyse durch.

DAS IST DNSWATCHGO:

Schutz außerhalb der Firewall

DNSWatchGo blockiert alle Verbindungsversuche zu böswilliger Infrastruktur, einschließlich Anfragen von Nutzern außerhalb des Netzes. Falls erforderlich, werden Sie umgeleitet.

Schulung der Mitarbeiter

DNSWatchGo ist die erste Sicherheitslösung auf dem Markt, die Phishing-Angriffe nicht nur unschädlich macht, sondern auch die Anwender in der Erkennung dieser Art des Angriffs schult.

Einfaches Management aus der Cloud

DNSWatchGO ist vollständig Cloud-basiert und benötigt keine Hardware oder Software-Updates. Rationalisierung der Implementierungs- und Verwaltungsprozesse spart Zeit und Geld.

Mehr Informationen unter: **watchguard.com/DNSWatchGO**

NO WAY TO FAR.

CSF Cyber Security Fairevent

Anfahrt

Messe Dortmund, Halle 8

Ihr Weg zum Cyber Security Fairevent

Anreise mit dem Auto

Sie haben direkten Anschluss über die B1 (A40) an die Autobahnen A1, A45, A2, A42 und A44. Bitte folgen Sie der Ausschilderung nach Dortmund und beachten Sie die Hinweisschilder der Messe Dortmund auf den Autobahnen.

Im Navigationsgerät geben Sie als Zieladresse „Im Rabenloh“ ein. Ab Zieladresse folgen Sie bitte den Ausschilderungen im Nahbereich zum Parkplatz A8 oder Parkhaus A1. Parkplätze in unmittelbarer Nähe stehen für ca. 8.800 Pkw zur Verfügung. Die Parkgebühren belaufen sich auf 7,00 EUR pro Pkw auf allen Parkflächen.

Zur besseren Orientierung nutzen Sie bitte den Geländeplan (s. o.).

Anreise mit dem Flugzeug

Die Entfernung vom Dortmunder Flughafen zu den Westfalenhallen Dortmund beträgt 12 km.
Der Düsseldorfer Flughafen ist 63 km entfernt, der Kölner Flughafen 96 km.

Öffentliche Verkehrsmittel

Vom Dortmunder Hauptbahnhof kommend, können Sie die U-Bahn-Linie 45 bis zur U-Bahn-Haltestelle „Westfalenhallen“ nutzen. Diese Haltestelle befindet sich im Osten des Messegeländes ca. 1 km von der Halle 8 entfernt.

Die zu Halle 8 nächstgelegene U-Bahn-Haltestelle liegt im Westen der Messe und ist mit der U42 Richtung „Grotenbachstraße“ bis Station „Theodor-Fliedner-Heim“ zu erreichen. Vom Hauptbahnhof kommend, nutzen Sie bitte die U45 Richtung „Westfalenhallen“, die U47 Richtung „Aplerbeck“ oder die U49 Richtung „Hacheney“ und steigen jeweils an der Station „Stadtgarten“ in die U42 Richtung „Grotenbachstraße“ um.

Die Westfalenhallen sind an den genannten Messe-Haltestellen ausgeschildert. Alle aufgeführten Haltestellen sind behindertengerecht.

Weitere Informationen zu Ihrer Anreise finden Sie hier:

Impressum

Unternehmen | Name des Unternehmers
Waveline-Mar.Com | Hasan Ezdi

Anschrift
Landsberger Straße 336
80687 München
Telefon: +49 (0) 89 124757-320
E-Mail: office@waveline-mar.com
Website: www.waveline-mar.com

Verfasser
Hasan Ezdi | Gastbeiträge der Medien- und Kooperationspartner

Gestaltung
Kristine Bruchmann, Hasan Ezdi

Druck
L.N. Schaffrath DruckMedien GmbH & Co. KG
Marktweg 42–50 | 47608 Geldern

Bildnachweise (entsprechend AGB/Nutzungsbedingungen)
Titel: @ Kovalenko/Fotolia | Fotos: @ Rich Carey/shutterstock, @ Vadim Sadovski/shutterstock, Gastbeiträge, privat

Erscheinungsjahr
2020


CSF Cyber Security Fairevent
Messe | Event | Kongress | Erlebniswelt
SEE YOU!
Dortmund, 04.–05. März 2020
2020
Dortmund, 03.–04. März 2021
2021
www.cybersecurity-fairevent.com