COMPLIANCE konkret

Das Kundenmagazin von Althammer & Kill
Ausgabe 4/2021

Patientendaten-Schutz-Gesetz: Der Gesetzgeber geht neue Wege.

Informationssicherheit wird in allen Krankenhäusern zur Pflicht!
Seite 6

Das Bildungswesen aus der Wolke
Digitales Schulwesen funktioniert nur mit angemessenen Konzepten.
Seite 10

Cyber-Angriffe auf Videokonferenzen
So schützen Sie sich vor unbefugten Zuhörern.
Seite 12

Über die Schulter geschaut
So wird eine organisationsweite Phishing-Kampagne organisiert, durchgeführt und ausgewertet.
Seite 16

News und Termine
Seite 4/5

Patientendaten-Schutz-Gesetz: Der Gesetzgeber geht neue Wege.
Informationssicherheit wird in allen Krankenhäusern zur Pflicht!
Seite 6

Das neue Telekommunikation-Telemedien-Datenschutz-gesetz ist da!
Die Umsetzung der ePrivacy-Richtlinie fordert die daten-schutzkonforme und sichere Gestaltung von Webpräsenzen.
Seite 9

Das Bildungswesen aus der Wolke
Digitales Schulwesen funktioniert nur mit angemessenen Konzepten.
Seite 10

Cyber-Angriffe auf Videokonferenzen
So schützen Sie sich vor unbefugten Zuhörern.
Seite 12

Erfolgsfaktoren der Krisenkommunikation
Diese acht Punkte sollten sie beherzigen.
Seite 14

Über die Schulter geschaut
So wird eine organisationsweite Phishing-Kampagne organisiert, durchgeführt und ausgewertet.
Seite 16

Kurz vorgestellt
Nina Hoffmann
Seite 19

Editorial

Liebe Leserin, lieber Leser,

Sie werden es sicherlich gemerkt haben – das Althammer & Kill Kundenmaga-zin zeigt sich im neuen Gewand und mit einem neuen Titel. Aus „Datenschutz konkret“ wird „Compliance konkret“. Wir begleiten unsere Mandanten seit Jahren vertrauensvoll bei der konformen Umsetzung der Themen Datenschutz und Informationssicherheit. Doch im Kern beraten wir seit jeher zu vielen weiteren Compliance-relevanten Themen. Wir sind daher sehr stolz, dass wir Mitte des Jahres den Bereich Cloud- & Cyber-Security auf eigene Beine gestellt und erfolg-reich platziert haben. Und auch der vierten Säule von Althammer & Kill, dem Bereich Compliance, haben wir einen neuen Anstrich verpasst.

Sie werden bei der Durchsicht der Lektüre außerdem feststellen, dass unsere Mitarbeiterinnen und Mitarbeiter stärker in den Fokus rücken. Neben den Ihnen bekannten Gesichtern – vor allem unsere Beraterinnen und Berater – arbeiten viele Personen im Hintergrund, die für den Beratungserfolg unverzichtbar sind. Schlussendlich ist eine erfolgreiche Beratung nur unter Mithilfe des gesamten Teams von Althammer & Kill möglich. Deshalb werden wir in den kommenden Ausgaben über die Schultern unserer Mitarbeiterinnen und Mitarbeiter schauen und Ihnen dadurch interessante Einblicke geben.

Im Namen des gesamten Unternehmens möchten wir uns bei Ihnen für die vertrauensvolle Zusammenarbeit im Jahr 2021 bedanken. Wir wünschen Ihrer gesamten Belegschaft, Ihren Familien, Freunden und Angehörigen eine besinn-liche Weihnachtszeit. Kommen Sie gesund und munter in das neue Jahr.

Thomas Althammer & Niels Kill

Darüber wird gesprochen

Diese und weitere aktuelle Themen sowie die Anmeldemöglichkeit für den Althammer & Kill-Newsletter finden Sie unter: *althammer-kill.de/aktuelles/news*

„Hallo Niedersachsen" bei Althammer & Kill
Am 17.11.2021 war das Fernsehen da: Anlässlich der Unterzeichnung eines Kooperationsvertrages des Landes Niedersachsen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Intensivierung des Schutzes vor Cyberattacken hat das populäre NDR-Regionalmagazin Thomas Althammer zum Thema „IT-Sicherheit" interviewt. Maximilian Klose konnte dem Team demonstrieren, wie leicht es ist, eine E-Mail-Phishing-Kampagne zu fahren.

„Hallo Niedersachsen" ist bis zum 17.11.2022 in der ARD Mediathek verfügbar. Link siehe QR-Code.

ConSozial 2021
Althammer & Kill sowie LearnBase waren im November auf der Fachmesse der Sozialwirtschaft „ConSozial" in Nürnberg vertreten. Wir danken allen Besucherinnen und Besuchern für spannende und intensive Gespräche!

Zahl des Monats

95 %

aller erfolgreichen Cyberattacken auf Unternehmen werden durch einen menschlichen Fehler möglich. Wir unterstützen Ihre Mitarbeitenden bei der Erkennung betrügerischer E-Mails!

Need-to-know-Prinzip – Mitarbeitende müssen und dürfen nicht alles wissen!
Zu den Grundlagen der Datenverarbeitung gehört unter anderem der Grundsatz der Integrität und Vertraulichkeit. Informationssicherheitsbeauftragte wissen damit umzugehen. Nicht jeder Mitarbeitende benötigt zur Erfüllung seiner Aufgaben zum Beispiel Einsicht in Personalakte, Kundendaten, Aufzeichnungen der Videoüberwachung oder Gesundheitsdaten!
althammer-kill.de/aktuelles/news/detail/need-to-know-prinzip-mitarbeitende-muessen-und-duerfen-nicht-alles-wissen

Zehn Bausteine zum ganzheitlichen Compliance-Management
Die Einhaltung ethischer Grundlagen und regulatorischer Vorgaben ist wesentlicher Bestandteil des Geschäftserfolgs. Sie planen die Etablierung eines ganzheitlichen Compliance-Programms in Ihrer Organisation?
althammer-kill.de/aktuelles/news/detail/zehn-bausteine-zum-ganzheitlichen-compliance-management

Veranstaltungen und Termine

Mehr Informationen, weitere Termine und Anmeldemöglichkeiten für unsere Veranstaltungen finden Sie unter: *althammer-kill.de/akademie/ueberblick*

02./03./09./10. Februar 2022 (halbtägig, 4 Tage)
Datenschutzkoordinator/in (DSGVO, DSG-EKD, KDG)
Mit dem Lehrgang zum Datenschutzkoordinator erwerben Sie das notwendige Grundlagenwissen, um Datenschutzbeauftragte bei deren Arbeit fachgerecht zu unterstützen und kompetenter Ansprechpartner zu sein. Am Ende des Seminars haben Sie die Möglichkeit, an einer Prüfung mit dem Zertifikatsabschluss „Datenschutzkoordinator" teilzunehmen. Dieses Zertifikat dokumentiert Ihre Datenschutzkompetenz gegenüber der Aufsichtsbehörde, Vorgesetzten, Geschäftspartnern und Mitarbeitenden Ihrer Organisation.

17. Februar 2022
Datenschutz in Online-Marketing und Social Media
Sie wollen wissen, was in den letzten 2 Jahren im Online-Datenschutz passiert ist, wann Cookie-Manager zwingend notwendig sind und was es bei ihrem Einsatz zu beachten gilt? Sie fragen sich, was es aktuell bei Plug-ins, E-Mail-Marketing, der Veröffentlichung von Fotos und der Nutzung von Social-Media-Kanälen zu beachten gibt? Sie zentralisieren Nutzerprofile in CRM-Systemen und analysieren Daten im Data-Warehouse? Ihr Dienstleister nimmt Ihnen vieles ab und Sie blicken nicht durch? Dann lohnt sich dieses Seminar!

Ihr Ansprechpartnerin für alle Themen rund um die Althammer & Kill-Akademie:

Nina Hoffmann
veranstaltungen@althammer-kill.de
Tel. +49 511 330603-0

23. Februar 2022
Workshop Verarbeitungsverzeichnis (DSGVO, DSG-EKD, KDG)
Sie möchten das notwendige Fachwissen für die Erstellung eines Verarbeitungsverzeichnisses nach DSGVO/ DSG-EKD oder KDG erhalten? Dann ist dieser Workshop genau das Richtige für Sie!

24. Februar/22. März 2022
Qualifizierung E-Learning-Coach
Sie haben bereits erste Erfahrungen mit E-Learning gesammelt? In der Qualifizierung zum E-Learning-Coach zeigen wir Ihnen auf, wie Sie Content auswählen und erstellen (Didaktik und Drehbuch) sowie Content umsetzen (Autorentools und zielgruppengerechte Lernangebote). Außerdem betrachten wir das E-Learning in der Praxis (Implementierung und Rahmenbedingungen).

08./09. März 2022 (ganztägig, 2 Tage)
ISO 27001 Foundation

1. Quartal 2022
Whistleblower-Richtlinie und Hinweisgebersystem

1. Quartal 2022
Wirksame Compliance für KMU und Gesundheits- und Sozialwesen

Die genauen Termine standen bei Redaktionsschluss noch nicht fest.

Patientendaten-Schutz-Gesetz: Diese Änderungen sind 2022 zu beachten.

IT-Sicherheitsvorfälle im Gesundheitswesen sind leider an der Tagesordnung. Nach erfolgreichen Angriffen auf Kliniken in Düsseldorf, Arnsberg und in anderen Städten müssen Vorkehrungen verschärft werden. Im Rahmen des Patientendaten-Schutz-Gesetzes (PDSG) wurde auch das Fünfte Sozialgesetzbuch angepasst. Diese Änderung hat auch Auswirkungen auf das Krankenhauszukunftsgesetz und die geplanten Fördervorhaben im kommenden Jahr.

Das Krankenhauszukunftsgesetz gliedert sich in elf Fördertatbestände. Obwohl diese inhaltlich grundverschieden sind, haben sie doch eins gemeinsam: der Gesetzgeber verlangt, dass mindestens 15 Prozent der jeweiligen Fördersumme (pro Fördertatbestand) in die Verbesserung der Informationssicherheit investiert werden. Fördertatbestand 10 widmet sich wiederum isoliert der Verbesserung der IT-Sicherheit in Krankenhäusern.

Bereits hier war abzusehen, dass IT- und Informationssicherheit in den kommenden Wochen, Monaten und Jahren beim Gesetzgeber einen höheren Stellenwert bekommt. Nicht zuletzt, weil seit einem Hackerangriff auf ein Klinikum in Düsseldorf im letzten Jahr die Meldungen von (versuchten) Cyberattacken auf das Gesundheitswesen nicht abgerissen sind. Der aktuelle Lagebericht des BSI verdeutlicht dies ebenfalls und lässt erahnen, dass Informationssicherheit, insbesondere in so sensiblen Bereichen wie dem Gesundheitswesen, nicht nur Spaß an der Freude ist. So geht aus dem Lagebericht 2021 des BSI hervor, dass die Anzahl neuer Schadprogramm-Varianten im Berichtszeitraum um 144 Millionen zugenommen hat (+22 %

Stichwort

Schutzziele

Zentrale Themen des branchenspezifischen Sicherheitsstandards für die Gesundheitsversorgung im Krankenhaus sind die bekannten vier Schutzziele nach ISO 27001:

- Verfügbarkeit
- Integrität
- Authentizität
- Vertraulichkeit

Der B3S ergänzt zwei weitere Ziele:

- Patientensicherheit
- Behandlungseffektivität

gegenüber dem Vorjahr). Besonders Ransomware macht Probleme. Diese verschlüsseln die Festplatten der Opfer und machen sie dadurch handlungsunfähig – erst durch Zahlung eines Lösegeldes ist ein „Weiterarbeiten" möglich. Was für „normale" Unternehmen ärgerlich bis hin zu existenzgefährdend ist, ist für Krankenhäuser bzw. deren Patientinnen und Patienten lebensgefährlich. Insofern ist es richtig und wichtig, dass der IT-Sicherheit von allen Krankenhäusern mehr Aufmerksamkeit gewidmet wird.

Doch das KHZG war und ist nicht das einzige Gesetz, welches in Sachen Datenschutz und IT- bzw. Informationssicherheit für Organisationen des Gesundheits- und Sozialwesens von Bedeutung ist. Auch das Patientendaten-Schutzgesetz (PDSG) dürfte im kommenden Jahr in den Fokus vieler IT- und Gesamtverantwortlichen rücken. Insbesondere für Krankenhäuser ist das PDSG von herausragender Bedeutung und wird umso wichtiger, wenn IT-Sicherheitsprojekte im Rahmen des KHZG beabsichtigt sind.

Patientendaten-Schutzgesetz und die Änderung des SGB V

Im Zuge des Patientendaten-Schutzgesetz (PDSG) wurde auch das Fünfte Sozialgesetzbuch (SGB V) angepasst. Neu hinzugekommen ist der Paragraf 75c SGB V – und dieser Paragraf ist für Krankenhausbetreiber richtig spannend! Denn mit dieser Änderung entstehen neue Anforderungen an die IT-Sicherheit in Krankenhäusern. Ab dem 1. Januar 2022 sind Krankenhäuser verpflichtet, angemessene technische und organisatorische Maßnahmen zu ergreifen, die gemäß dem Stand der Technik geeignet sind um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie weiterer Schutzziele zu vermeiden.

Hierzu stehen den Krankenhäusern branchenspezifische Standards zur Verfügung. Einer dieser branchenspezifischen Standards ist der „Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus", ausgearbeitet von der Deutschen Krankenhausgesellschaft (DKG). Im Oktober 2019 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Sinne des BSI-Gesetzes diesen Standard für geeignet erklärt und in die Liste der branchenspezifischen Sicherheitsstandards (B3S) aufgenommen.

IT-Sicherheit an einem Sicherheitsstandard ausrichten

Doch galt diese Vorgabe nicht schon längst? Die Antwort lautet: „Ja"! Allerdings nur für Krankenhäuser, die unter die Definition der Kritischen Infrastruktur fallen (> 30.000 Fälle p. a.). Auf Krankenhäuser mit einer Fallzahl < 30.000 kommen neue Anforderungen entgegen. Und das sind eben diese Krankenhäuser, die im Rahmen des KHZG von Fördermitteln profitieren können. Erstmalig sind diese Krankenhäuser gesetzlich verpflichtet, ihre IT-Sicherheit an einen Sicherheitsstandard auszurichten und alle zwei Jahre zu evaluieren bzw. an den „Stand der Technik" anzupassen.

Der branchenspezifische Sicherheitsstandard für die Gesundheitsversorgung (B3S) drängt sich folgerichtig nahezu auf. Um die Umsetzung möglich zu machen, bedarf es Experten, die im Umgang mit und der Implementierung von IT-Sicherheitsstandards geübt sind. Dies bedeutet einen erhöhten Personalaufwand und damit höhere Kosten.

Stichwort

ISMS

Ein Informationssicherheitsmanagementsystem (ISMS) ist ein System von Vorgaben und Abläufen – es definiert Regeln und Methoden, um die Informationssicherheit in der Organisation dauerhaft sicherzustellen. Hierbei werden gesetzliche Anforderungen berücksichtigt und entsprechend in das Managementsystem eingearbeitet.

Aufbau eines Informationssicherheits-managementsystem (ISMS)

Wenn nicht bereits geschehen, sollte zeitnah mit dem Aufbau eines Informationssicherheitsmanagementsystems (ISMS) unter Berücksichtigung des krankenhausspezifischen B3S-Standards begonnen werden. Für Krankenhäuser, die bereits ein dokumentiertes ISMS vorweisen können, sollte geprüft werden, ob dieses mit den Anforderungen des § 75c SGB V bzw. mit dem Branchenstandard korreliert. Abweichungen, wie zum Beispiel das Fehlen der Schutzziele „Patientensicherheit" und „Behandlungseffektivität", sind zu korrigieren. &

Das neue Telekommunikation-Telemedien-Datenschutzgesetz ist da!

Seit Jahren geistert die ePrivacy-Richtlinie durch die Köpfe der Datenschützer und Marketingverantwortlichen. Nach mehreren Jahren des Wartens wird die ePrivacy-Richtlinie nun in einem nationalen Gesetz umgesetzt: Das Telekommunikation-Telemedien-Datenschutzgesetz (oder kurz: TTDSG).

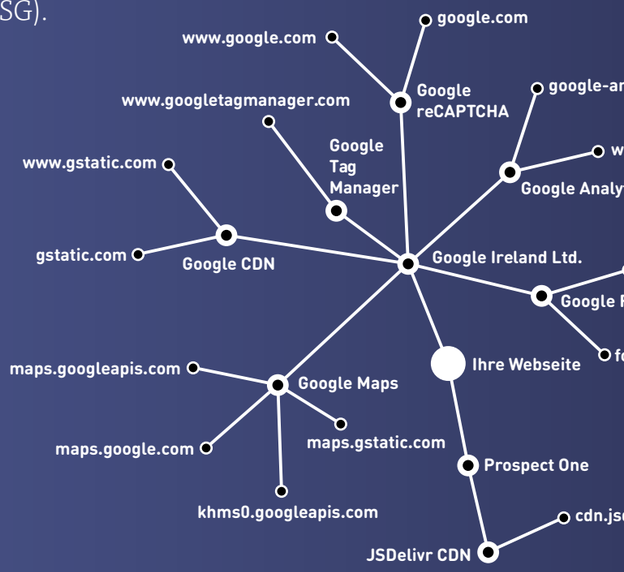
Das TTDSG stellt unter anderem klar, dass das Speichern von und der Zugriff auf Informationen in der Endeinrichtung eines Endnutzers grundsätzlich nur mit einer DSGVO-konformen Einwilligung erlaubt ist, welche derzeit und wohl zukünftig im Online-Verkehr hauptsächlich über „Cookies" geregelt wird.

Mit Blick auf die Cookies soll mit dem TTDSG eine nutzerfreundliche und auch wettbewerbskonforme Einwilligungsverwaltung erreicht werden, welche anerkannten wie anzuerkennenden Verwaltungs-Dienstleistungen (bekannt als „Cookie-Management" bzw. „Consent-Management"), Internetbrowser und Telemedienanbieter einbeziehen soll. Und auch andere Rechtsprechungen wie das Schrems II-Urteil und die damit verbundenen Hürden für die Übermittlung von personenbezogenen Daten in Drittstaaten wie den USA sind beim Betreiben von Webseiten zu berücksichtigen.

Was ist zu tun?

Nahezu jede Organisation, die eine Website betreibt, wird sich an den Vorgaben des TTDSG und den allgemeinen Anforderungen der DSGVO orientieren müssen. Grund genug die eigenen Webpräsenzen und Webapplikationen hinsichtlich des Datenschutzes und der Datensicherheit auf den Prüfstand zu stellen.

Unsere Cloud- & Cyber-Security Experten überprüfen im Kundenauftrag die rechtskonforme und sichere Gestaltung von Webseiten und Webapplikationen. Neben der rein analytischen Auswertung erhalten unsere Kunden aussagekräftige Ergebnisberichte und Handlungsempfehlungen, um Datenschutz- und Datensicherheitslücken pragmatisch und wirksam abstellen zu können. Und auch bei der Umsetzung stehen wir unseren Kunden vertrauensvoll mit Rat und Tat zur Seite. &



In der Grafik oben ist dargestellt, welche ausgehenden Verbindungen auf einer Webseite vorhanden sind. In diesem Beispiel ist der Verbindungsaufbau zu einem großen Dienstleister aus den USA besonders auffällig. Die Rechtmäßigkeit muss spätestens mit dem TTDSG überprüft werden.

Brauchen Sie Unterstützung?

Möchten auch Sie Ihre Webseiten und Webapplikationen einem rechtlichen und technischen Test unterziehen? Sprechen Sie uns hierzu gerne an!

Sören Hartmann
vetrieb@althammer-kill.de
Tel. +49 511 330603-0

Das Bildungswesen aus der Wolke

Die Corona-Pandemie hat der Digitalisierung im Bildungswesen Vorschub geleistet. Dies könnte sich diesen Winter endlich auszahlen, sollten die Schülerinnen und Schüler wieder in den Wechsel- oder Distanzunterricht gehen müssen. Doch wo Licht ist, da ist auch Schatten. So wurde erst kürzlich von Sicherheitslücken in Schul-Apps berichtet. Diese Vorfälle zeigen: Die Digitalisierung der Bildung funktioniert nur mit angemessenem Management des Datenschutzes und der Informationssicherheit. Und einem Bewusstsein für Security-relevante Themen bei jedem Kultusministerium, jeder Schulleitung und jeder Lehrkraft.

Von einer aus Dresden stammenden Schul-App sollen Daten von 400.000 Schülerinnen und Schülern (E-Mail-Adresse, Geburtsdatum, Standort) im Netz auffindbar gewesen sein. In der diesbezüglichen Pressemitteilung des App-Herstellers steht geschrieben, dass im gemeinsamen Austausch mit dem sächsischen Datenschutzbeauftragten die Lücke geschlossen wurde und der Hersteller bis Ende des Jahres mehrere Maßnahmen zum Daten- und Jugendschutz plant.

Ein datenschutzrechtliches Nachspiel wird die Lücke wohl nicht haben; der sächsische Datenschutzbeauftragte habe laut Medienberichten bisweilen keinen Verwaltungsakt erlassen. Was auf den ersten Blick verständlich wirkt (Sicherheitslücken werden gefunden und anschließend geschlossen) – liest sich bei näherer Betrachtung allerdings etwas anders. Die Sicherheitslücke wurde von den Sicherheitsexperten des Kollektivs „zerforschung“ entdeckt. Nach einer 30-tägigen Disclosure-Phase fand Ende Oktober 2021 das Public Disclosure statt. Das Kollektiv listet in diesem Public Disclosure neben zahlreichen Datenschutz- und Informationssicherheits-Missständen auch Jugendschutzmängel auf. Neben der Zugriffsmöglichkeit auf die Daten der Nutzerinnen und Nutzer sei es möglich gewesen, ungehindert in Chatgruppen minderjähriger Schülerinnen und Schüler einzutreten und an den Diskussionen teilzunehmen. Außerdem sollen sich aus den Gruppen- bzw. Chatbezeichnungen teilweise besondere Kategorien personenbezogener Daten, die unter den Artikel 9 DSGVO fallen, abgeleitet haben. Eine Moderation dieser Gruppen & Chats sei dem Kollektiv nicht ersichtlich gewesen. Außerdem habe es in der App Persönlichkeitstests, Quizze und Mini-Spiele gegeben. Diese dienten der Profilbildung, um gezielt Werbung für Ausbildungs- und Studienplätze von Partnern in der Umgebung auszuspielen.

Das sollten Verantwortliche und Software-Hersteller beachten

Was für Verantwortliche und Software-Hersteller bei der Erstellung, Implementierung und Nutzung von Software gilt, gilt für Anbieter und Nutzer von Bildungsclouds und School-Applikationen umso mehr. Der Datenschutz und die Informationssicherheit müssen einen hohen Stellenwert im Projekt genießen. Immerhin verarbeiten diese Lösungen eine große Anzahl an personenbezogenen Daten von Schülerinnen und Schülern – viele der betroffenen Personen sind minderjährig. Gleichermaßen werden höchst persönliche Bewertungen verarbeitet, die außerhalb der relevanten Lehrerschaft keinem Dritten offenbart werden dürfen.

Das oben aufgeführte, abschreckende Beispiel des Datenlecks verdeutlicht, wieso von Anfang an Expertinnen und Experten in Sachen Datenschutz und Informationssicherheit bei der Entwicklung und Implementierung um Rat gefragt werden sollten. Gemäß den Veröffentlichungen von „zerforschung“ verteidigte sich der App-Hersteller mit der Behauptung, man hätte als Startup nicht die Möglichkeit, sichere Software zu entwickeln. „Man solle aber jungen, deutschen Startups eine Chance geben, sich gegen große Konzerne zu behaupten“ – so zumindest soll es der zuständige Geschäftsführer dem Kollektiv gegenüber geäußert haben. Wenn es um den Schutz von Kindern und Jugendlichen geht, sollte dies jedoch kein akzeptables Argument darstellen dürfen. Erfolg und Sicherheit schließen sich nicht gegenseitig aus – im Gegenteil. Privacy und Security gewinnen ständig an Bedeutung und werden längst als zentrale Bausteine des Marketings verwendet.

Was können Verantwortliche in Bildungseinrichtungen also tun, um die Bildung weiter zu digitalisieren und zeitgleich sicherer zu gestalten?

1. Security bereits bei der Planung berücksichtigen
Wie bei der Einführung von zentraler IT üblich, wird zu Beginn eines jeden Projektes eine Strategie erarbeitet. Verantwortliche und Software-Hersteller sollten sich die Fragen stellen, welches Problem (z. B. Distanzunterricht) mit welchen Lösungen (z. B. Bildungsclouds, kommerziellen Applikationen usw.) begenet werden soll. Der Vollständigkeitshalber sollte bereits in dieser Phase die Frage nach der Sicherheit gestellt werden. Dies kann aufwendige Nachbesserungen verhindern.

2. (Security-)Experten bei der Umsetzung eng mit einbinden
Es hat sich bewährt regelmäßige Penetrationstests der Applikation(en) durchführen zu lassen – bestenfalls zeitgleich mit der Programmierung der Software. So können bereits in der Entwicklungsphase Lücken und Schwachstellen identifiziert und behoben werden. Dies mindert einen nachträglichen Aufwand massiv.

Bei der Einführung bestehender (und kommerzieller) Systeme sollten Datenschutz- und Informationssicherheitsexperten zu Rate gezogen werden. Getreu dem Motto „Vertrauen ist gut, Kontrolle ist besser“ sollten die Datenschutz- und Informationssicherheits-Versprechen des Herstellers auf Plausibilität überprüft werden. Darüber hinaus ist eine möglichst datenschutzfreundliche Konfiguration der Systeme herzustellen und die gesetzlichen Dokumentationspflichten (z. B. die Datenschutz-Folgenabschätzung) einzuhalten. Wichtig zu wissen: Nicht alle Landesdatenschützer dulden (ohne weiteres) den Einsatz von amerikanischen bzw. außereuropäischen Dienstleistern an Bildungseinrichtungen. Hier gilt es die aktuelle Rechtsprechung und vorherrschende Meinung im Blick zu behalten. Hardware-seitig muss die sichere Implementierung auf den vorhandenen IT-Gerätschaften nachhaltig sichergestellt werden und die gesamte Implementierung in das ggf. bestehende Informationssicherheitsmanagementsystem (ISMS) eingearbeitet werden.

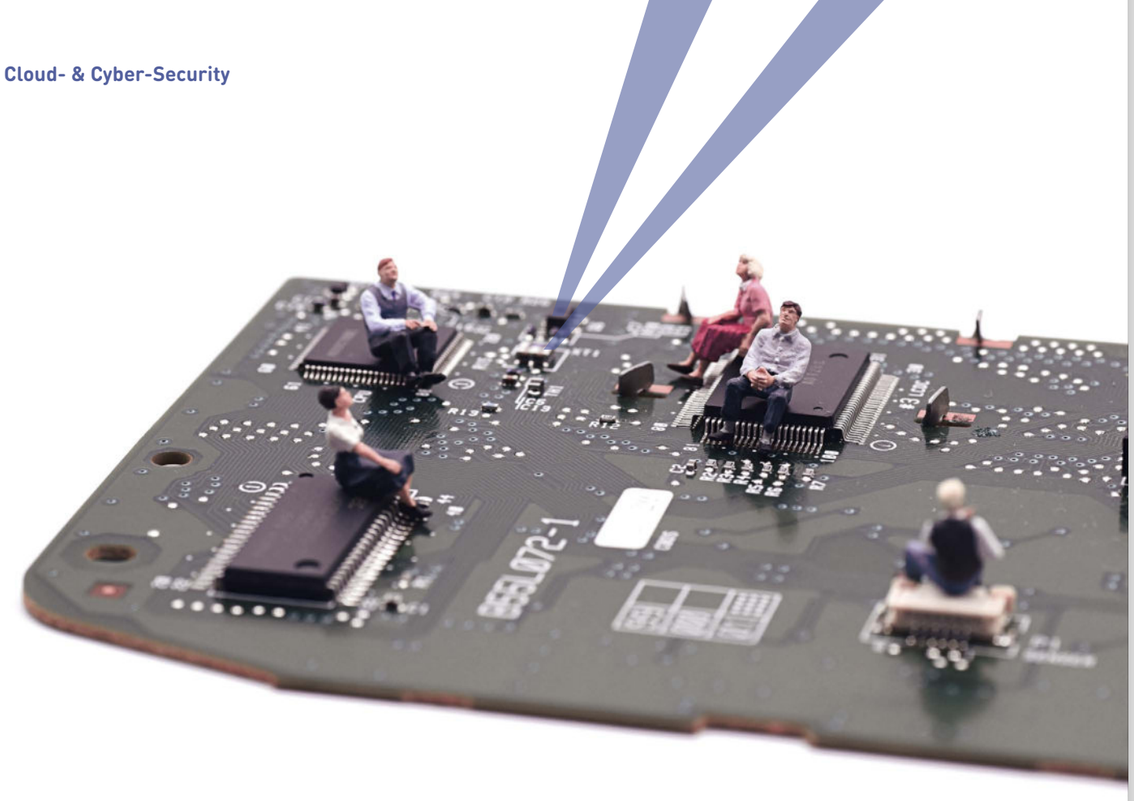
Datenschutz und Informationssicherheit sind nur Momentaufnahmen

Erfolgreich eingeführte Systeme benötigen über die Einführung hinaus datenschutzrechtliche und informationssicherheitstechnische Betreuung. Zum einen können sich durch Rechtsprechungen neue Sachverhalte ergeben, die in der datenschutzrechtlichen Risikobetrachtung zu würdigen sind. Zum anderen verändert sich die Bedrohungslage in der IT ständig. Neben der rein technischen Sicherheit sollte auch die Security-Awareness der Belegschaft nachhaltig aufgebaut werden. Denn je sicherer Systeme werden, desto mehr rückt der Faktor Mensch in den Fokus von Cyber-Kriminellen. Dieser Trend ist schon lange zu beobachten. Es ist daher höchste Zeit, neben einer technischen auch eine personelle Resilienz gegenüber Cyber-Attacken herzustellen. &

In eigener Sache

Althammer & Kill durfte die eigene Expertise bei der Entwicklung der Niedersächsischen Bildungscloud unter Beweis stellen. Die Niedersächsische Bildungscloud (NBC) ist ein Projekt in Trägerschaft der Landesinitiative n-21: Schulen in Niedersachsen online e. V.

Althammer & Kill wurde im Rahmen der Entwicklung der Niedersächsischen Bildungscloud für die Beratung und Begleitung der Datenschutz-Folgenabschätzung sowie der Erstellung eines Datenschutzkonzeptes hinzugezogen. Nach Finalisierung des Datenschutzkonzeptes und der Datenschutz-Folgenabschätzung ist die Niedersächsische Bildungscloud ein datenschutzrechtliches Erfolgsmodel. Weitere Bundesländer werden folgen. Und auch dort wird auf die Expertise von Althammer & Kill zurückgegriffen werden.



Cyber-Angriffe auf Videokonferenzen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ihren turnusmäßigen Bericht „Lage der IT-Sicherheit in Deutschland“ für das Jahr 2021 veröffentlicht. Auffällig: Cyber-Angriffe steigen weiter dramatisch an. Besonders besorgniserregend sind dabei die Cyber-Angriffe auf Videokonferenzsysteme. Wieso genau diese Systeme beliebte Angriffsziele sind und was sich hinter dem Begriff Credential Stuffing verbirgt, erfahren Sie in diesem Beitrag.

Viele Organisationen haben ihre interne und externe Kommunikation auf Videokonferenzen umgestellt. Ein Großteil der Organisationen tat dies nicht zwingend freiwillig, sondern wurde durch die Corona-Pandemie in die Virtualisierung der Arbeitsplätze getrieben. Dies blieb auch Cyber-Kriminellen nicht verborgen. Videokonferenzsysteme wurden somit zu einem attraktiven Ziel für Cyber-Kriminelle. Das BSI beobachtete hierbei, dass das Interesse der Angreifenden in der Beschaffung von Informationen aus privaten Konferenzen bestand. Insofern gilt es für Arbeitnehmerinnen und Arbeitnehmer sowie für Privatpersonen gleichermaßen aufmerksam zu sein. Einmal entwendete Zugangsdaten werden oftmals auf Plattformen verkauft und z. B. im Rahmen des Credential Stuffing ausgenutzt.

Credential Stuffing

Beim Credential Stuffing werden „erlangte“ Anmeldeinformationen (engl. „Credentials“) fremder Personen auf verschiedenen Plattformen ausprobiert. Der Grundgedanke dahinter ist logisch: Angreifer hoffen, dass sich die Opfer mit denselben Anmeldeinformationen auf verschiedenen Plattformen registriert haben. Im Kontext der Videokonferenzsysteme wird es dahingehend spannend, dass sich mittels des Credential Stuffing Angreifende in Videokonferenzen einwählen können, ohne durch eine Zugangsbeschränkung daran gehindert zu werden. Die Angreifenden haben schlicht und ergreifend „gültige Ausweispapiere“. So ist es dann möglich, weitere Informationen abzugreifen und gegen die teilnehmenden Personen oder gegen Organisationen zu verwenden; bspw. im Rahmen von Erpressungen und Wirtschaftsspionage.

Wirksame Schutzmechanismen

Nur wenn Personen bekannt ist, welche Angriffsszenarien in der Realität existieren, können wirksame Schutzmechanismen aufgebaut werden. Die beliebteste (und wohl erfolgversprechendste) Art und Weise, um an Anmeldeinformationen zu gelangen, ist weiterhin das sogenannte Phishing. Hier erhält das Opfer im Vorhinein eine gut gefälschte E-Mail, in der es angeregt wird, auf eine scheinbar legitime URL zu klicken.

Das Opfer merkt hierbei nicht, dass es auf eine „gefälschte“ Seite gelotst wird. Dort angekommen sollen die eigenen Zugangsdaten eingetragen werden – meist unter einer fadenscheinigen Begründung, die jedoch auf den ersten Blick plausibel erscheint. Das perfide hierbei: heutige Phishing-Mails sind kaum von „legitimen“ E-Mails zu unterscheiden.

Security-Awareness Kampagnen

Durch Social Media, zahlreiche Datenleaks in der Vergangenheit und viele weitere Faktoren können Phishing-Angriffe mittlerweile sehr zielgerichtet erfolgen. Die Streuverluste werden für die Angreifer immer geringer. Im Internet existieren große Datenbanken, die Kunden- bzw. E-Mail-Listen von globalen Anbietern enthalten. Anhand derer können mit geringstem Aufwand passgenaue Phishing-Kampagnen nachgebaut werden.

Als äußerst effektive Schutzmaßnahme hat das regelmäßige Durchführen von Security Awareness Kampagnen erwiesen. Dabei werden Phishing- und Social Engineering-Attacken so realitätsnah wie möglich simuliert. Auf Seite 16-18 beschreibt Ihnen unser Cloud- & Cyber-Security-Experte Maximilian Klose wie eine Phishing-Kampagne ablaufen kann, welche Ergebnisse beim erstmaligen Durchführen zu erwarten sind und wie dadurch die Awareness nachhaltig aufrechterhalten wird.

„Die Nutzung der Multi-Faktor-Authentifizierung sichert Systeme wirksam ab. 99 % aller Angriffe können so abgewehrt werden! “

Simon Lang
Produktmanager

Multi-Faktor-Authentifizierung

Des Weiteren sollte von der Multi-Faktor-Authentifizierung (MFA) Gebrauch gemacht werden. Selbst wenn unbewusst die eigenen Zugangsdaten abhandengekommen sind, kann der Angreifer auf die mit MFA geschützten System nicht zugreifen, da er (in den meisten Fällen) nicht im Besitz des zweiten Faktors ist. Multi-Faktoren lassen sich grundsätzlich in drei Kategorien unterscheiden:

- Etwas, was Du weißt (z. B. Passwörter, ...)
- Etwas, was du bist (z. B. Fingerabdruck, Gesicht, ...)
- Etwas, was du hast (z. B. Hardwaretoken, Smartcard, ...)

Hierbei bildet die Kombination aus mindestens zwei der drei Kategorien die Multi-Faktor-Authentifizierung; also beispielsweise das eigene Passwort + ein Hardwaretoken. Doch nicht alle „Faktoren“ sind gleichermaßen geeignet. Anrufe oder SMS als zweiter Faktor gehören langsam aber sicher der Vergangenheit an und werden durch Hardwaretoken, biometrische Merkmale, Authentifikator-Apps usw. verdrängt. &

Tipps vom Admin: Air-Gapped Backup

Backups sind eine wichtige Stütze für den Notfall. Dabei sollten Backups möglichst auf mehreren Medien gespeichert werden. Zudem sollten Backups immer verschlüsselt sein.

Mindestens ein Backup sollte getrennt, also offline, von allen Systemen gespeichert werden, sog. Air-Gapped Backups. Systeme, die nicht verbunden sind, können quasi nicht gehackt werden. Sie sollten an sicherer Stelle, z. B. im Tresor oder einer Bank, verwahrt werden. Wichtig: Auch hier können Dinge schiefgehen! Festplatten oder Bänder gehen defekt oder werden beim Transport gestohlen.

Erfolgsfaktoren der Krisenkommunikation

Unabhängig davon, ob im Umgang mit Verschlüsselungstrojaner, Datenschutzverletzung, Compliance-Vorfall oder eines sonstigen Krisenereignisses in der Organisation: professionelle Krisenkommunikation folgt entlang bestimmbarer Grundprinzipien. Wir haben acht wichtige Erfolgsfaktoren zur wirksamen Prävention zusammengefasst. Doch zuvor schauen wir zurück und zeigen auf, wieso Krisenkommunikation ein elementarer Baustein des Compliance-Managements ist.

Ein wirksames Compliance-Management soll Rechtsverstöße verhindern und Schaden von der Organisation abwenden. Dabei muss der Schaden nicht immer monetärer Art sein – auch das Image kann unter negativer Berichterstattung leiden. Der Fall AWO Frankfurt zeigt eindrücklich, dass unzureichende Kontrollmechanismen nicht nur einen Millionenschaden verursachen können, sondern für einen langen Zeitraum negative mediale Berichterstattung nach sich zieht. Und er beweist auch, dass der Satz „Bad Publicity is better than no publicity" schlichtweg falsch ist.

Fehler nicht wiederholen

Das wahre Ausmaß des Skandals kam erst Schritt für Schritt zum Vorschein. Vorausgegangen war ein Bericht des Hessischen Rundfunks über ein überhöhtes Gehalt der Ehefrau des Frankfurter Oberbürgermeisters. Neben dem überhöhten Gehalt soll die Leiterin einer Kindertagesstätte der AWO auch einen Firmenwagen bezogen haben – wohl zu Unrecht. Fortlaufende Recherchen offenbarten darüber hinaus, dass sich die AWO-Kreisverbände Wiesbaden und Frankfurt überhöhte Gehälter und Honorare

in Rechnung gestellt haben. Und auch die Stadt Frankfurt gilt mittlerweile als Geschädigte in diesem Fall. So soll die AWO Dienstleistungen für die Betreuung von Flüchtlingen in Rechnung gestellt haben, die sie jedoch nicht erbracht habe. Der genaue Vorwurf kann aus zahlreichen Medienportalen entnommen werden. Dieser Fall zeigt jedoch deutlich, dass der Aufbau eines wirksamen Compliance-Managementsystems nicht nur für DAX-Konzerne von großer Bedeutung ist. Auch gemeinnützige Organisationen können Opfer von rechtswidrigen Handlungen werden und ohne wirksame Compliance-Strukturen bleiben solche Handlungen mitunter jahrelang unentdeckt.

Doch auch detailliert ausgearbeitete Compliance-Management-Systeme verhindern unlautere Handlungen der Mitarbeitenden nicht zu 100 Prozent. Wichtig ist es daher, geeignete Kanäle zur Aufdeckung und Kommunikation von Comppliance-Vorfällen zu schaffen. Zur Aufdeckung solcher Handlungen bietet sich die Etablierung eines Hinweisgebersystems an. Oftmals decken Kolleginnen und Kollegen ein Fehlverhalten auf, wissen jedoch nicht, wo und an wen der Verdacht gemeldet werden kann. Die Angst vor Repressalien ist groß. Insbesondere, wenn es sich bei der Person um den eigenen Vorgesetzten handelt. Ein Hinweisgebersystem schützt Mitarbeiterinnen und Mitarbeiter vor solchen Situationen und hilft zudem, schwerwiegende Sachverhalte intern aufzuklären, bevor diese an die Öffentlichkeit dringen. Wenn Informationen jedoch an die Öffentlichkeit durchgestochen wurden, ist eine kluge Krisenkommunikation gefragt.

Krisenkommunikation richtig gestalten

Mit diesen acht Erfolgsfaktoren sind Sie im Fall der Fälle für die schwierige Kommunikation nach außen gewappnet.

1. Mit einer Stimme sprechen
Außenkommunikation im Krisenfall sollte über eine einzelne, definierte Stelle der Organisation oder des Unternehmens erfolgen. Dies kann z.B. die Kommunikationsabteilung oder der Pressesprecher sein, zuweilen auch ein Mitglied der Geschäftsführung oder des Vorstands. Unabgestimmte Äußerungen aus verschiedenen Quellen können Unglaubwürdigkeit, Spekulationen oder Gerüchte verursachen oder die Organisation juristisch angreifbar machen. Dies sollte dringendst verhindert werden.

2. Transparenz
Krisenereignisse fordern Offenheit und Ehrlichkeit. Die Umdeutung von Sachverhalten sollte unbedingt vermieden werden. Das Nennen konkreter Maßnahmen sowie Hilfs- und Unterstützungsangebote und zuverlässig einzuhaltende Zeitpunkte der Umsetzung sollten fokussiert werden.

3. Betroffenheit
Auch wenn es selbstverständlich klingt; angemessenes Mitgefühl und ehrliche Betroffenheit sollten glaubwürdig signalisiert werden.

4. Frühzeitige Kommunikation
Eine proaktive Informationspolitik zahlt sich aus und bildet Vertrauen. Bereits in ruhigen Zeiten sollten relevante Krisenszenarien sowie die von Seiten der Organisation getroffenen Präventionsmaßnahmen kommuniziert werden. Wenn es zu einer Krisensituation kommt, ist es frühzeitig notwendig die Öffentlichkeit, Partner oder Kunden zu informieren. Die Kommunikation sollte hierbei ruhig, durchdacht und transparent erfolgen.

5. Konflikte
Konflikte mit den Medien, der Öffentlichkeit, Partnern oder Kunden sollten unter allen Umständen vermieden werden. Sollte es dennoch Konflikte geben, sind diese intern zu klären und nicht in der Öffentlichkeit.

6. Transparente interne Kommunikation
Relevante Mitarbeitende sind transparent zu informieren. Für die Mitarbeitende und das Stimmungsbild in der Belegschaft ist es unvorteilhaft, wenn diese relevante Informationen von außerhalb oder aus den Medien erfahren. Mitarbeitende sind zudem Multiplikatoren innerhalb der Organisation oder im persönlichen Umfeld.

7. Geschwindigkeit
Im Ernstfall ist bei der Krisenkommunikation, neben der Offenheit und Ehrlichkeit, auch Schnelligkeit und Geschwindigkeit ein weiterer entscheidender Faktor. Ein typisches Risiko ist die zu späte öffentliche Reaktion und der damit einhergehende Vertrauensverlust.

8. Debriefing & Lessons Learned
Professionelle Nachbereitung hilft, um Schwachstellen und Fehler zu erkennen und die Prozesse präventiv für weitere Krisen zu verbessern. Deshalb sollten auch niedrigschwellige Vorfälle mit den intern relevanten Personen detailliert aufgearbeitet werden. Fragen wie „Was ist gut gelaufen? Was sollte verbessert werden? Bei welchen Aspekten und Themen sollte künftig anders vorgegangen werden?" sind nun wichtig und bedürfen einer ausführlichen Antwort. &

Das Cloud- & Cyber-Security-Team bei der Arbeit

Maximilian Klose ist Berater für Cloud- & Cyber-Security.
Im Kundenauftrag versuchen er und seine Kolleginnen und Kollegen,
an sensible Informationen der auftraggebenden Organisation zu gelangen.
Dazu werden verschiedenste Methoden angewandt – je nach Einsatzszenario.

Das Repertoire besteht aus individuellen Phishing-Kampagnen sowie Security-Checks und Penetrationstests von einzelnen Webseiten bis hin zu gesamten Netzwerken. Ihr erklärtes Ziel ist es, Lücken und Schwachstellen aufzudecken, bevor diese von böswilligen Angreifern entdeckt werden. Maximilian Klose berichtet über eine durchgeführte Phishing-Kampagne, deren Ergebnisse und die daraus abgeleiteten Maßnahmen.

Hallo Maximilian, Ihr habt bei einer großen Organisation eine Security-Awareness-Kampagne durchführen. Was war das Ziel?

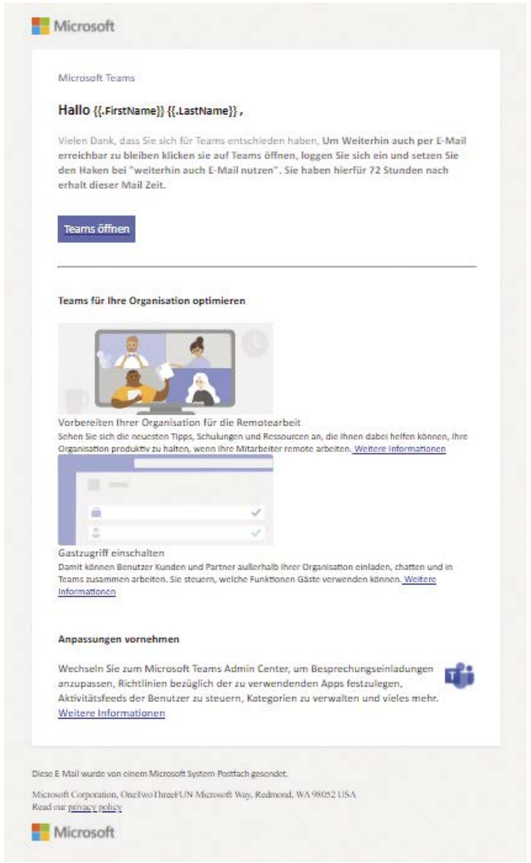
Maximilian Klose: Zunächst einmal muss festgehalten werden, dass die meisten erfolgreichen Angriffe durch menschliche Fehler möglich werden. Dessen ist sich unser Kunde bewusst. Wir sollten in Erfahrung bringen, wie es um das Sicherheitsbewusstsein in der Organisation bestellt ist. Langfristig soll die Sicherheit und Resilienz durch aufgeklärte Mitarbeitende nachhaltig verbessert werden. Wir möchten einen Prozess etablieren, um die “Security Awareness” über den Kampagnenzeitraum hinaus sicherzustellen. Im konkreten Fall haben wir im ersten Schritt eine Phishing-Kampagne aufgesetzt. Wir wollten schauen, ob und wenn ja, wie viele Personen auf eine gefälschte E-Mail hereinfallen und dazu verleitet werden, ihre persönlichen Zugangsdaten preiszugeben.

Bevor wir zum Ergebnis kommen: Wie seid Ihr das Projekt angegangen? Habt Ihr einfach loslegen können oder gab es vorab notwendige Absprachen mit dem Kunden?

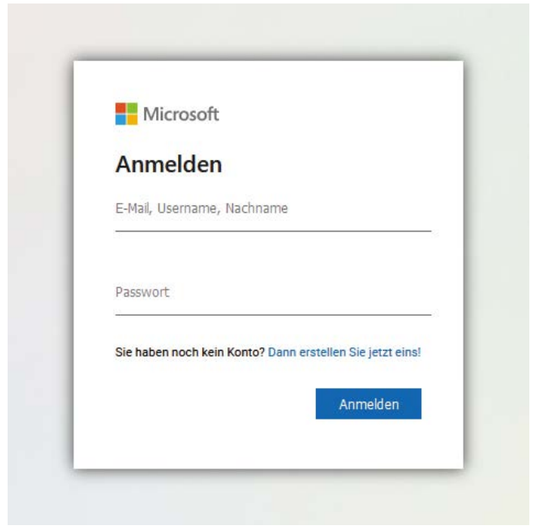
Maximilian Klose: Ja es gibt vorher Absprachen und diese sind auch sehr wichtig! Es ist auf jeden Fall darauf zu achten, dass wir gemeinsam mit dem Kunden einen Scope festlegen. Zudem ist es von enormer Bedeutung, einige Personen in verantwortlicher Rolle einzuweihen. Gemeinsam mit den Verantwortlichen legen wir fest, welche Dienste wir „phishen“. Dabei sollte der Kreis der Eingeweihten allerdings so klein wie möglich bleiben.

Die Bandbreite dessen, was wir anbieten können, ist sehr groß – von Microsoft 365-Landingpages bis hin zu spezifischen Login-Seiten von typischer Branchensoftware, Intranet-Seiten usw. Natürlich sollten bei der Auswahl plausible Dienste ausgewählt werden. Genau an diesem Punkt wird die Absprache mit den verantwortlichen Personen enorm wichtig.

Beim vorliegenden Projekt wurde der Scope auf die Zugangsdaten für Microsoft 365 und die im Einsatz befindliche Kundenverwaltungssoftware der Organisation gelegt. Nachdem uns schlussendlich die E-Mail-Adressen über einen sicheren Kanal übermittelt wurden, konnte es auch schon losgehen.



Schritt 1: Gefälsche Phishing-E-Mail

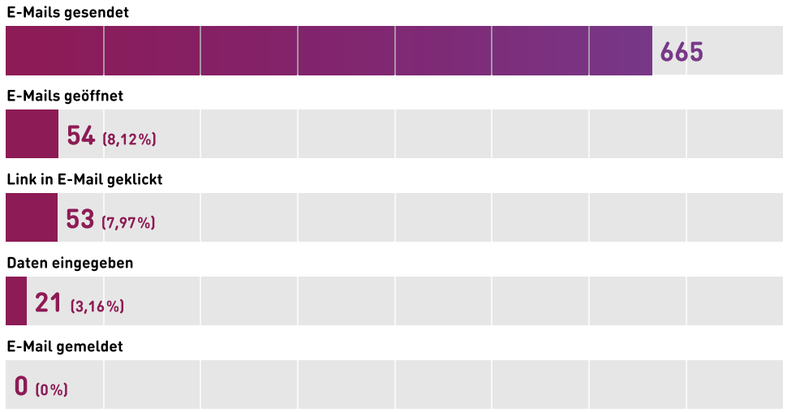


Schritt 2: Gefälsche Login-Seite

Wenn Ihr die Phishing-Seiten individuell gestalten könnt, wie kann man dann schlussendlich Eure Seiten von echten Seiten unterschieden? Lasst Ihr den Mitarbeitenden überhaupt eine Chance?

Maximilian Klose: Wir versuchen schon, detailgetreue Nachbauten von Login-Seiten zu erzeugen. Allerdings bauen wir kleinere Fehler ein, anhand derer ein aufmerksamer User erkennen kann, dass es sich um eine Falle handelt. Wir wollen schlussendlich genau das erreichen: Das User auf Signale achten und gefälschte Webseiten von echten, sicheren Webseiten unterscheiden können.
Im Übrigen liegen uns eine Vielzahl von gefälschten Mails aus der „freien Wildbahn“ vor, anhand derer wir uns orientieren können. Die allermeisten besitzen Fehler: zum Beispiel in der Rechtschreibung, in der Optik oder sind gänzlich veraltet. Wir versuchen diese Fehler so gut es geht zu adaptieren, um möglichst authentische Ergebnisse zu erhalten.

Um Deine Frage zu beantworten: Selbstverständlich lassen wir den Mitarbeitenden eine Chance – wir orientieren uns allerdings stark an der Realität. Und die Realität ist nun einmal, dass gefälschte Seiten zwar nicht perfekt sind, aber immer besser werden. Das müssen wir bei unserer Tätigkeit berücksichtigen.



Ergebnisse der Phishing-Kampagne

Zurzeit befindest Du dich in der Abschlussphase des Projektes. Kannst du uns einen Ausblick geben, wie „erfolgreich" eure Kampagne lief?

Maximilian Klose: Die Durchführungsphase lief für uns sehr gut und natürlich sind wir auch stolz, wenn wir messbare Ergebnisse produzieren. Zur Wahrheit gehört aber auch, dass traurigerweise viele Mitarbeitende auf unsere Mails hereingefallen sind – mehr als wir vermutet hatten und das stimmt uns nachdenklich.

Für die Organisation haben wir definitiv Handlungsbedarfe identifiziert, die wir nun aufarbeiten und mit dem Kunden besprechen werden. Allerdings war es für den Kunden und dessen Mitarbeitenden die erste Kampagne dieser Art.

Ich bin mir sicher, dass bereits diese Kampagne für Awareness gesorgt hat, sodass wir beim nächsten Mal andere Ergebnisse erwarten dürfen.

Wie werden die Ergebnisse aufgearbeitet und präsentiert? Und was sind Folgemaßnahmen, die getroffen werden sollten?

Maximilian Klose: Die Ergebnisse werden statistisch aufgearbeitet. Wir werden unserer auftraggebenden Organisation keine Rohdaten zur Verfügung stellen und fungieren als eine Art Treuhänder auch in Absprache mit dem Betriebsrat.

Der Schutz der Mitarbeitenden steht bei allen Beteiligten ebenso an oberster Stelle, wie die organisationsweite Sicherheit. Deshalb erhält unser Kunde einen Ergebnisbericht mit aggregierten Daten. Aus diesem wird zum Beispiel ersichtlich, wie hoch der prozentuale Anteil der „Gephishten" ist – wer im Einzelnen betroffen war, werden wir aber unter keinen Umständen preisgeben.

Als Datentreuhänder sind wir uns der vertrauensvollen Rolle, insbesondere den Mitarbeitenden gegenüber, voll bewusst! Den Ergebnisbericht präsentieren wir anschließend vor der Geschäftsleitung und den verantwortlichen Personen in der Organisation. Im Gespräch werden wir weitere Awareness-Maßnahmen festlegen, um die Sensibilisierung langfristig sicherzustellen. Dazu eignen sich regelmäßige Sensibilisierungsformate mittels E-Learning, prominent platzierte Plakate usw. Irgendwann im Laufe des nächsten Jahres wird es dann eine weitere Phishing-Kampagne geben. An dieser werden wir uns hoffentlich die Zähne ausbeißen.

Vielen Dank für die interessanten Einblicke in Eure Arbeit! &

Impressum

Redaktion/V. i. S. d. P.:
Danny Sellmann, Thomas Althammer
Haftung und Nachdruck: Die inhaltliche Richtigkeit und Fehlerfreiheit wird ausdrücklich nicht zugesichert. Jeglicher Nachdruck, auch auszugsweise, ist nur mit vorheriger Genehmigung der Althammer & Kill GmbH & Co. KG gestattet.
Gestaltung: Ralf Winternheimer
winternheimer.net
Fotos Mini-Figuren: Katja Borchhardt
miniansichten.de
Anschrift:
Althammer & Kill GmbH & Co. KG
Roscherstraße 7 · 30161 Hannover
Tel. +49 511 330603-0
althammer-kill.de
Schutzgebühr Print-Ausgabe: 5,– €

Die Menschen hinter Althammer & Kill:

Nina Hoffmann

Ja hallo, wer bist du denn?

Nina Hoffmann: Hi, ich bin Nina, 27 Jahre jung, komme aus Wunstorf und habe einen Master in Betriebswirtschaftslehre an der Universität Bremen absolviert. In meiner Freizeit bin ich leidenschaftlich aktiv im Fahrsport und besitze noch ein eigenes Pferd.

Wie lange arbeitest du schon bei Althammer & Kill?

Nina Hoffmann: Bei Althammer & Kill bin ich jetzt seit zwei Jahren.

Was sind Deine Aufgaben?

Nina Hoffmann: Ich bin bei uns im Hause für die Verwaltung und Organisation zuständig und leite unsere Akademie.

Was steckt alles hinter der Althammer & Kill-Akademie?

Nina Hoffmann: In unserer Akademie bieten wir verschiedene Seminarformate rund um unsere Themensäulen Datenschutz, Informationssicherheit, Cloud- und Cyber-Security sowie Compliance und zu unserer E-Learning Plattform LearnBase an. Alle zwei Wochen findet ein kostenloses, einstündiges Webinar zum Reinschnuppern in das jeweilige Thema statt. Unsere Online-Seminare haben eine Dauer von einem halben bis zu 4 Tagen und können auch als Inhouse-Seminare gebucht werden.

Wie wurden die Online Seminare von den Kunden angenommen?

Nina Hoffmann: Die Pandemie hat auch uns gezwungen neue Wege einzuschlagen, sodass wir unser gesamtes Seminarprogramm in den Online-Bereich verlegt haben. Dies hat durchaus auch zu anfänglichen, technischen Schwierigkeiten geführt, die wir aber erfolgreich gemeistert haben und nun fast noch lieber im digitalen Geschäft unterwegs sind. Unsere Kunden freuen sich dabei über wegfallende Reisezeiten und wir sind stets bemüht, den persönlichen Kontakt durch interaktive Elemente und kleine Gruppen sowie Workshops aufrecht zu erhalten.

Wie können dich unsere Kunden erreichen?

Nina Hoffmann: Per E-Mail bin ich über veranstaltung@althammer-kill.de erreichbar, sowie telefonisch unter 0511 330603-0. Da ich Frühaufsteher bin, ist die Wahrscheinlichkeit, mich vormittags zu erreichen sehr hoch 😊.

Was gibt es 2022 Neues von der Akademie?

Nina Hoffmann: Für das kommende Jahr sind neue Seminarformate in Planung, insbesondere zum Thema Cyber-Security, aber auch zu unserem Steckenpferd, dem Datenschutz. Dabei testen wir immer wieder, welche Wochentage und Seminardauern sich für unsere Kunden am besten eignen und sind bemüht zu variieren. Dabei helfen uns insbesondere die ausgefüllten Feedbackumfragen unserer Seminarteilnehmenden, an dieser Stelle ein großes Dankeschön an diejenigen, die uns wertvolle Hinweise und Bewertungen gegeben haben. Wir wollen weiterhin digitale Seminare anbieten, da die weitere Entwicklung der Corona-Pandemie noch abzuwarten bleibt und wir kein Risiko für unsere Kunden und Kollegen eingehen wollen. &

ALTHAMMER & KILL

Digitalisierung sicher gestalten

Althammer & Kill bietet pragmatische Lösungskonzepte für Datenschutz und Digitalisierung. Wir beraten bundesweit im Umfeld Datenschutz, Informationssicherheit, Cloud- und Cybersecurity und Compliance.

Unsere rund 40 Mitarbeitenden an den Standorten Hannover, Düsseldorf und Mannheim sind als externe Datenschutzbeauftragte, Informationssicherheits- und IT-Experten für mehr als 500 Kunden unterschiedlichster Branchen tätig.

Althammer & Kill GmbH & Co. KG

Roscherstraße 7 · 30161 Hannover · Tel. +49 511 330603-0
Mörsenbroicher Weg 200 · 40470 Düsseldorf · Tel. +49 211 936748-0
Kaiserring 10–16 · 68161 Mannheim · Tel. +49 621 121847-0

vertrieb@althammer-kill.de
althammer-kill.de

ISO 9001:2015

Mitgliedschaften

NIEDERSACHSEN DIGITAL · BvD e.V. MITGLIED · FINSOZ · GDD MITGLIED