CYBERCRIME

Eine Risikoanalyse
für mittelständische
Unternehmen

INHALTSVERZEICHNIS

EXECUTIVE SUMMARY

HOMEOFFICE – REMOTE WORK ALS RISIKOFAKTOR

2020 war ein großer Katalysator für die Digitalisierung in deutschen Unternehmen: Remote Work wurde ausgebaut, Mitarbeiter ins Homeoffice geschickt, die IT-Infrastruktur zunehmend dezentralisiert. Das hatte drei Dinge zur Folge:

- Zum einen **destabilisierten sich so IT-Landschaften**, deren Sicherheitseinrichtungen nur auf zentralisierte Arbeitslandschaften ausgelegt waren.
- Weiter wurden **digitale Kommunikations- und Kollaborationstool**s eingeführt oder ausgebaut – jedoch oft ohne die notwendigen Sicherheitsmaßnahmen, um schnell Infrastruktur zur Weiterarbeit bereitzustellen.
- Und zuletzt **schwächt die dezentrale Arbeitsweise den Kontakt** Ihrer Mitarbeiter zueinander. Denn erstaunlicherweise hat sich gezeigt, dass der Vor-Ort-Austausch die Wahrscheinlichkeit senkt, auf eine Phishing-Mail hereinzufallen.

*Quelle: https://www.faz.net/aktuell/wirtschaft/digitec/mehr-hacker-angriffe-auf-kliniken-und-kritische-infrastruktur-17062421.html

MITTELSTAND – PHISHING-ATTACKEN AUF VAPS NEHMEN ZU

Angriffe auf Mittelständler erfolgen anders als bei großen Konzernen. Während dort eher die VIPs – also das obere Management – im Kreuzfeuer von Phishing-Attacken stehen, werden Angriffe auf mittelständische Unternehmen breiter gestreut.

Mitarbeiter, die als Very Attacable Persones („besonders leicht angreifbare Personen") gelten, werden gezielt angegangen. Die Auswahl dieser besonders vulnerablen Ziele ist vielversprechender und führt unkomplizierter zu einem schnellen Erfolg der Angreifer.

Dies liegt an der besonderen Struktur des (deutschen) Mittelstands: Das Unternehmen befindet sich in eigener Hand, man ist mit seinen Vorgesetzten (bis hin zum Geschäftsführer) sowie den Kollegen vertraut. Dies führt einerseits zu einem Klima des Vertrauens – fatalerweise leider auch in die eigene IT-Sicherheit.

KRITIS – ZIELE MIT HOHER GESELLSCHAFTLICHER RELEVANZ

Trotz schärferer Anforderungen an die IT-Sicherheit von KRITIS-Unternehmen wurden bis Anfang November 2020 141 erfolgreiche Cyberangriffe gemeldet. Davon 43 auf Gesundheitsdienstleister. 2019 waren es im Berich der kritischen Infrastruktur noch 121, 2018 sogar lediglich 62 erfolgreiche Versuche.* Neben dem Gesundheitswesen sind Energie- und Wasserversorger, Banken und Versicherungen betroffen. Meist handelt es sich bei derartigen Vorfällen um sog. Ransomware-Angriffe, die eine Lösegeldforderung zur Entschlüsselung von Daten nach sich ziehen. Aufgrund ihrer Kritikalität erhoffen sich Angreifer schnelle und hohe Lösegeldzahlungen, um eine schnelle Betriebswiederaufnahme herzustellen.

CYBERKRIMINALITÄT

WIE AKUT IST DIE BEDROHUNGSLAGE IN DEUTSCHLAND?

Cyberkriminalität richtet sich gegen Privatpersonen und in besonderem Maße auch gegen Firmen und Organisationen bzw. Institutionen.

Die größte Gefahr geht hierbei von Identitätsdiebstahl infolge einer Preisgabe von personenbezogenen Daten aus. Dies gelingt häufig durch den Einsatz sog. Phishingmails. Deren Schadpotenzial ist in Folge der Corona-Krise gestiegen: Die Agentur der Europäischen Union für Cybersicherheit (ENISA) etwa vermeldet einem Anstieg von Phishing-Mails um mehr als 600 % im vergangenen Jahr.** Cyberattacken, die auf menschliche Mithilfe setzten, waren und sind in der Corona-Krise besonders erfolgreich.

Doch warum ist das so? Und insbesondere, wie können Sie sich und Ihr Unternehmen gegen derartige Angriffe erfolgreich absichern?

*Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Jahreslageberichte/jahreslageberichte_node.html
**Quelle: https://www.enisa.europa.eu/publications/phishing

DIE BEDROHUNGSLAGE HAT SICH 2020 VERSCHÄRFT

Die Corona-Krise sorgt für Verunsicherung in großen Teilen der Bevölkerung. Denn weder privat, beruflich noch politisch waren wir auf eine derartige Situation vorbereitet. Und nicht nur das: Die neue Situation erforderte plötzlich und quasi über Nacht neue Lösungen für ein weiteres Funktionieren unserer Gesellschaft sowie unseres Arbeitslebens. Dies bot uns viele Chancen bei der Digitalisierung, eröffnete jedoch auch neue Angriffsflächen für Cyberkriminalität.

DIGITALISIERUNG: KATALYSATOR FÜR CYBERANGRIFFE

2020 war ein großer Katalysator für die Digitalisierung in deutschen Unternehmen: Remote Work wurde ausgebaut, Mitarbeiter ins Homeoffice geschickt, die IT-Infrastruktur zunehmend dezentralisiert. Das hatte drei Dinge zur Folge: Zum einen destabilisierten sich so IT-Landschaften, deren Sicherheitsmaßnahmen nur auf Vor-Ort-Arbeit ausgelegt waren. Weiter wurden digitale Kommunikations- und Kollaborationstools eingeführt oder ausgebaut – jedoch oft ohne die notwendigen Sicherheitsmaßnahmen, um schnell Infrastruktur zur Weiterarbeit bereitzustellen. Und zuletzt schwächt die dezentrale Arbeitsweise den Kontakt Ihrer Mitarbeiter zueinander. Denn erstaunlicherweise hat sich gezeigt, dass der Vor-Ort-Austausch die Wahrscheinlichkeit senkt, auf eine Phishing-Mail hereinzufallen.

PHISHING & SOCIAL ENGINEERING

Bei Phishing-Mails handelt es sich um betrügerische E-Mails, die den Empfänger zu selbstschädigenden Handlungen bewegen sollen. Dies umfasst etwa das direkte Abgreifen von Passwörter und Zugangsdaten oder aber die Installation einer Schadsoftware durch die Hilfe der User. Um ihr Ziel zu erreichen, setzen die Angreifer auf Social Engineering-Techniken. Dies meint die böswillige Manipulation von Personen

DIE ZAHL DER CYBERANGRIFFE IN DEUTSCHLAND WAR 2020 AUF EINEN NEUEN HÖCHSTSTAND. LAUT BKA ERHÖHTE SICH DIE ZAHL DER TATEN UM MEHR ALS 15 % IM VORJAHRESVERGLEICH AUF 100.514.***

***Quelle: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2020/Presse2020/200930_pmBLBCybercrime.html

mittels psychologischer Tricks, um Schaden bei diesen und oder deren verbundenen Unternehmen anzurichten. Darunter fallen etwa die Ausnutzung von Ängsten, (beruflichen) Zwängen oder Notlagen.

Die Motive für derartige Betrugskampagnen sind vielfältig: Angefangen bei der Bereicherung durch Lösegelderpressung nach Datenverschlüsselung, bis hin zur langfristige Schädigung von (Konkurrenz-) Unternehmen durch Spionage, Sabotage oder Streufeuer.

DER FAKTOR MENSCH ALS GRÖSSTER RISIKOFAKTOR

So banal das klingt: Die Interaktion mit betrügerischen Telefonanrufen, gefakten Social Media Anfragen, schädlichen E-Mails oder Webseiten ist DIE Sicherheitslücke in Ihrem IT-System. Um Ihr Unternehmen erfolgreich zu kompromittieren, braucht es die (aktive) Mithilfe des Mitarbeiters: Betrügerische und gefährliche Schadsoftware

MEHR ALS 99 % ALLER ATTACKEN ERFORDERN MENSCHLICHE INTERAKTION.*

*Quelle: https://www.proofpoint.com/de/newsroom/press-releases/human-factor-report-2019-proofpoint-report-zeigt-99-prozent-aller

DIESE BETRUGSFORMEN SOLLTEN SIE KENNEN

PHISHING („FISHING FOR PASSWORDS“)

Betrügerische E-Mails, die der Bereicherung des Senders dienen, indem sie den Empfänger zu selbstschädigenden Handlungen verleiten – vorrangig durch das Abgreifen von Identitätsmerkmalen oder das Einschleusen von Mal-/Spy- oder Ransomware zum Eindringen in ein (Firmen-)Netzwerk.

VISHING („VOICE PHISHING“) & SMISHING („SMS-PHISHING")

Betrügerische Telefonanrufe und SMS, die darauf abzielen, wichtige Accountdaten und Identifikationsmerkmale abzugreifen. Besonders Vishing dient auch oft der Informationsgewinnung zu wichtigen Entscheidungsträgern. Ein Cyberattacke wird im Nachgang mit den gewonnenen Informationen durchgeführt.

SPEAR PHISHING & WHALING

Eine Sonderform des Phishings, die sehr zielgerichtet auf Personen im oberen Management oder auf kritische Informationen im Unternehmen (Finanzen, Patente, Geschäftsgeheimnisse) abzielt.

(CALL-)ID SPOOFING

Ein Hacker fälscht hierbei die Identität einer Person oder Behörde, um so vermeintlich seriöse Anrufe abzusetzen oder E-Mails zu verfassen. So werden täuschend echte (aber gefälschte) Mailaccounts erstellt, tatsächliche Mailaccounts mittels Schadsoftware übernommen oder die Displayanzeige von Telefonanlagen aus der Ferne manipuliert. ID Spoofing zielt vorrangig auf Informationsgewinn für weitere kriminelle Handlungen.

BUSINESS EMAIL COMPROMISE (BEC)/ CEO FRAUD/ IDENTITY THEFT

Ein großes, aber noch immer unterschätztes Risiko für Unternehmen ist der sog. CEO Fraud. Hierbei täuschen Betrüger die Identität des CEOs (oder anderer wichtiger Manager) vor, um Druck auf Mitarbeiter auszuüben. So sollen diese etwa schnelle Zahlung veranlassen oder geheime interne Informationen weitergeben. Die benötigten Informationen sind oft online verfügbar (Impressum, Presseberichte oder Social Media) oder wurden durch Vishing/Phishing-Kampagnen in Erfahrung gebracht.

wird von modernen Systemen zuverlässig erkannt. Daher setzen Betrüger nun auf die Manipulation derjenigen Komponente, die sich nicht hinter einer technischen Absicherung verbirgt: dem Menschen.

Leider werden derartige Betrugsmaschen immer besser und können selbst von geschulten Usern nicht mehr unbedingt auf den ersten Blick als solche erkannt werden. Der unbekannt-verschollene, reiche Verwandte aus absurdesten Teilen der Welt wurde mittlerweile abgelöst von täuschend echt aussehenden z. B. PayPal-E-Mails, die gezielt die Passwörter und Kreditkartendaten der Nutzer ab-„fischen" wollen.

Auch schlechte Grammatik und falsches Vokabular finden sich in modernem, gut gemachtem Malware-Spam kaum noch. Auch ein https-Link ist laut BSI* längst keine Garantie mehr für Sicherheit – in etwa 60 %

DIE GRÖSSTE GEFAHR FÜR KMU GEHT VON IDENTITÄTSDIEBSTAHL & MALWARE AUS (RANSOMWARE/ SPYWARE), HIER IST FAST IMMER MENSCHLICHE INTERAKTION IM SPIEL.

*Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf

des registrierten Malware-Spams in 2019/20 kommen bereits https-Links zum Einsatz. Zwar soll das Security-Zertifikat sichere Homepages ausweisen, doch kann man dieses kostenlos im Internet lizenzieren lassen. Unabhängig davon, ob der Inhalt tatsächlich für den Verbraucher sicher ist.

MODERNER (MALWARE-)SPAM NUTZT UNSERE SCHWÄCHEN AUS

Dies sind meist emotionale Gründe wie Leistungs- und Zeitdruck. Oder menschliche Routinen wie Müdigkeit und somit Unachtsamkeit am Morgen. Oftmals wird auch ein unmittelbarer Bezug zum Empfänger und somit hohe Relevanz vorgetäuscht. Oder aber es werden Heuristiken und Automatismen der Personen ausgenutzt (kundensupport@arnazon.de). Berufliche Zwänge in Kombination mit emotionaler Aktivierung sorgen ebenfalls für eine hohe Klickrate (z. B. ein unzufriedener „Kunde").

96 % DER DEUTSCHEN UNTERNEHMEN HABEN 2019/20 EINEN GESCHÄFTSSCHÄDIGENDEN CYBERANGRIFF ERLITTEN.*

*Quelle: https://industrie.de/it-sicherheit/96-prozent-deutscher-unternehmen-haben-mindestens-einen-cyberangriff-erlitten/

DIE PSYCHOLOGIE HINTER SOCIAL ENGINEERING

DRUCK & ANGST

HILFSBEREITSCHAFT

AUTORITÄT

NEUGIERDE

LOB & SCHMEICHELEI

BEDÜRFNIS NACH INFORMATION

VERTRAUEN & INTIMITÄT

ÜBERRUMPLUNG & MANIPULATION

DER MITTELSTAND IM VISIER

ANGRIFF AUF VAPS STATT VIPS

Angriffe auf Mittelständler erfolgen anders als bei großen Konzernen. Während dort eher die VIPs – also das obere Management – im Kreuzfeuer von Phishing-Attacken stehen, werden Angriffe auf mittelständische Unternehmen breiter gestreut.

Mitarbeiter, die als Very Attacable Personas („besonders leicht angreifbare Personen") gelten, werden angegangen: Das sind zumeist neue Mitarbeiter, aber auch Finanzabteilungen oder noch unerfahrene Admins mit erweiterten Rechten.

Die hohe Erfolgsquote derartiger Angriffe liegt an der besonderen Struktur des (deutschen) Mittelstands: Das Unternehmen befindet sich in eigener Hand, man ist mit seinen Vorgesetzten (bis hin zum Geschäftsführer) sowie den Kollegen vertraut. Dies führt einerseits zu einem Klima des Vertrauens – fatalerweise leider auch in die eigene IT-Sicherheit.

Zum anderen versprechen sich Angreifer einen höheren und schnelleren Need, eine Lösegeldzahlung zu begleichen. Das liegt zum einen an der geringeren Liquidität kleinerer Unternehmen, für die und deren Inhaber ein Stillstand existenzgefährdend sein kann, andererseits auch an den kürzeren Entscheidungswegen bei einfacheren hierarchischen Strukturen.

UNAUFGEKLÄRTE MITARBEITER

Dass mittelständische Unternehmen eine höhere Anzahl an VAPs haben als große Unternehmen, liegt auch an der mangelnden Aufklärung der Mitarbeiter. Aufgrund der Größe (und der damit vermeintlichen geringen Angriffsfläche) wiegen sich Mittelständler in falscher Sicherheit. Und sparen z. B. bei Mitarbeiterschulungen zu Phishing und Social Engineering.

SCHWACHE IT-SECURITY-INFRASTRUKTUR

Geringere Ausgaben für die eigene interne IT bedeuten auch ein kleineres Budget für notwendige Sicherheitsmaßnahmen wie Backups, höhere Sicherheitsstufen und Notfallpläne zur Abwehr und Schadensbegrenzung bei Cyberangriffen. Oftmals fehlt schon der wichtigste Basisschutz in Form von Multifaktor Authentifizierung.

MITTELSTÄNDLER IM FOKUS VON CYBERKRIMINALITÄT

„Wir sind zu klein – das lohnt sich gar nicht", dieser Trugschluss vieler KMUs wird oft sehr teuer. Denn das BKA sieht bereits seit Jahren einen akuten Anstieg an Cyberangriffen auf kleine und mittelständische Unternehmen. Besonders im Krisenjahr haben Attacken zugenommen, und auch die Qualität dieser hat sich geändert.

Das hat auch etwas damit zu tun, dass sich der Ort geändert hat, an dem wir arbeiten. Das remote Setup im Homeoffice hat neue Schwachstellen in der IT-Infrastruktur sichtbar gemacht, wie die mangelhafte Absicherung von privaten Netzwerken. Durch die räumliche Trennung der Mitarbeiter werden Angriffe zudem – wenn überhaupt – erst spät bemerkt oder berichtet. Das gilt nicht nur für die Berichterstattung an die IT, sondern auch für den täglichen Austausch vor möglichen neuen Gefahren.

Und Phishing-Mails sind nach wie vor das Einfallstor für kriminelle Aktivitäten. Dennoch würde es zu kurz greifen, technische Barrieren zu ignorieren und nur auf Mitarbeitertrainings zu setzen. Wir zeigen Ihnen im Folgenden, warum.

*Quelle: https://www.bitkom.org/sites/default/files/file/import/181008 Bitkom Studie Wirtschaftsschutz 2018 NEU.pdf

GENÜGEN MITARBEITERSCHULUNGEN?

Leider nein! Denn es genügt ein Mitarbeiter, der einen Link oder Anhang öffnet, um in Ihr System einzudringen.

Dennoch ist die gezielte Schulung Ihrer Mitarbeiter ein erster Schritt zur Prävention derartiger Angriffe. Etwa zu den Themen Phishing/ Social Engineering, um sie für diese Themen zu sensibilisieren. Gleichzeitig gehören verbesserte Back-up-Strukturen mit häufigeren und sog. Offline-Back-ups (d. h. Back-ups, die nicht aus dem Netzwerk heraus änderbar sind) zu einem Vorsorgeplan gegen Cyber-, insbesondere Ransomware-Angriffe. Sie müssen jedoch bedenken, dass eine mögliche Veröffentlichung gestohlener Daten DSGVO-Klagen nach sich ziehen.

ORGANISATIONALE MASSNAHMEN & PROZESSE

Grundlage für die erfolgreiche Umsetzung aller nicht-technischen Maßnahmen gegen Phishing-Angriffe ist, Ihre Unternehmensprozesse so zu gestalten, dass ein Identitätsmissbrauch quasi ausgeschlossen werden kann. Hierzu zählen etwa ein 4-Augen-Prinzip bei Finanztransaktionen oder ein eingeschränktes Zugriffsmanagement zu kritischen Systemen.

Daneben müssen Sie klare Kommunikationsregeln etablieren. Dies umfasst zentrale und flächendeckende Regelungen über die Verwendung von E-Mails, Intranet oder anderer interner wie externer Kommunikations- und Kollaborationstools. Zum anderen die Frage, an wen ein Phishing-Verdacht gemeldet werden soll. Der Aufbau einer positiven Sicherheitskultur ist entscheidend, damit Mitarbeiter proaktiv und angstfrei verdächtige Aktivitäten sowie eigene Fehler melden.

ONLINEAUFTRITTE KRITISCH BELEUCHTEN

Unternehmen und deren Mitarbeiter sind heute notwendigerweise auf vielen Plattformen präsent. Dennoch sollten Sie hinterfragen, welche Informationen über Ihr Unternehmen und Ihre Mitarbeiter frei verfügbar sind – und welche dieser Informationen es besser nicht sein sollten.

Setzen Sie sich aktiv mit Ihren Online- und Social Media-Auftritten auseinander und erarbeiten Sie einen Code of Conduct sowie Guidelines zu den Social Media Auftritten Ihres Unternehmens und ihrer Mitarbeiter.

MITARBEITER SCHULEN

Mitarbeiter sind Ihr Kapital – auch, wenn es um Ihre IT-Sicherheit geht. Denn ohne Interaktion mit dem Menschen kommen heutige Cyberattacken kaum in Ihr System, da – bei der nötigen Pflege – die Systeme intelligent Schadsoftware erkennen können.

Daher sollten Sie nicht am falschen Ende sparen und in (Simulations-)Trainings zu den Themen Phishing und Social Media investieren. Hierzu gibt es verschiedene Ansätze, die Sie intern oder mit externen Dienstleistern durchführen können. Hierunter fallen etwa Simulationen & „Dry Runs" zu internen fingierten Phishing Angriffen, Konzepte für Initialtraining neuer Mitarbeiter sowie für laufende Maßnahmen aller Kollegen, Seminare bzw. Webinare oder Web Based Trainings sowie E-Learning-Tools. Hier sollte jedoch eine wiederholte Re-Sensibilisierung stattfinden, weshalb klar definierte, kleinere und sich wiederholende Einheiten sinnvoller sind als groß angelegte und komplizierte Initiativen.

FOLGEN VON PHISHING FÜR IHR UNTERNEHMEN

AUSFALL DES KOMPLETTEN BETRIEBS

FINANZIELLER VERLUST/ ÜBERWEISUNGSBETRUG

DATENVERLUST/ DATENVERSCHLÜSSELUNG

VERÖFFENTLICHUNG VON VERTRAULICHEN DATEN

DSGVO-VERSTÖSSE NACH DATENDIEBSTÄHLEN

REPUTATIONS-VERLUST

Ursache: Kompromittierung von Zugangsdaten/ Konten

SOCIAL ENGINEERING

RANSOMWARE-INFEKTION

SONSTIGE MALWARE-INFEKTION

TECHNISCHE BARRIEREN

SCHÜTZEN, AUCH WENN DER MENSCH VERSAGT

EIN BEISPIEL*

Oktober 2020: Hacker konnten im Rahmen einer Phishing-Kampagne Daten zu Mitarbeiteraccounts von Schweizer Hochschulen ab-phishen. Die so gewonnenen Informationen nutzten sie zur gezielten Änderung von Empfängerkonten für Lohnzahlungen im Personalsystem/ Personalstammdaten im System. Es entstand ein Schaden im sechsstelligen Bereich.

Die Etablierung einer effektiven, technischen Hürde in Form von Multifaktor Authentifizierung zur Änderung wichtiger Stammdaten hätte menschliches Versagen ausgleichen können.

*Quelle: https://www.it-daily.net/shortnews/25650-hacker-stehlen-sechsstellige-summe-von-schweizer-hochschulen

TECHNISCHE BARRIEREN SIND DAS A UND O FÜR EINE SICHERE UNTERNEHMENS-IT

Sicherheitssoftware entwickelt sich ständig weiter: Heutige Anti-Virus und Anti-Malwareprogramme funktionieren meist proaktiv, d. h. die ihr zugrunde liegenden Algorithmen sind in der Lage, auch neue, noch unbekannte Schadsoftware anhand bestimmter Heuristiken zu identifizieren. Und zu blockieren oder löschen, bevor diese Schaden anrichten kann.

ETABLIEREN SIE GRUNDLEGENDE TECHNISCHE SICHERHEITSMASSNAHMEN

Regelmäßige und zeitnahe Updates aller Betriebssysteme, Server- und Anwendungssoftware erhöhen die grundsätzliche Sicherheit Ihrer Systeme. Denn es gibt kaum eine Software auf dem Markt, die nicht mit Bugs oder Sicherheitslücken im Code ausgeliefert wird. Alte und bekannte Bugs sind ein gern genutztes Ziel für Angreifer; dagegen hilft nur die Installation der vom Hersteller bereitgestellten Patches.

Neuere, oft noch unbekannte Fehler sind hingegen meist (noch) kein lohnendes Ziel: Die Suche nach den aktuellsten, neuartigen Schwachstellen (im Wettlauf mit den Herstellern) ist sehr aufwendig und für sich genommen zunächst nicht lukrativ genug. Daher setzen Angreifer weniger auf interne, technische Schwachstellen, sondern auf eine einfach zu überlistende externe Schwachstelle – den User vor dem PC.

DIE SCHWACHSTELLE MENSCH

Bevor man zu diesem gelangt, gibt es noch einen technischen Schwachpunkt, der gekonnt überwunden werden muss: der automatisierte Malware-Scanner unserer E-Mail-Postfächer: Verbirgt sich hier ein gefälschter Link, der auf eine Website führt, auf der sich Schadsoftware befindet, oder die Mitarbeiter dazu auffordert, ihre Daten dort einzugeben, kann dieser sie (logischerweise) nicht erkennen.

Genau diese technische Lücke nutzen Angreifer, um an ihr Ziel zu gelangen: Sie setzen darauf, dass das System nicht erkennt, dass der dahinterliegende Inhalt für den User schädlich ist.

Eine klug aufbereitete und stimmig formulierte Phishing Mail führt oft genug – trotz vermeintlicher Aufklärung – dazu, dass ein Mitarbeiter den Anweisungen folgt und

einen Link oder einen Anhang öffnet: Und somit unwissentlich eine Brücke für die Angreifer schlägt, indem er dort Handlungen vornimmt, die Ihre Sicherheitssysteme überlisten.

Haben Angreifer erst das Passwort eines Mitarbeiters, können sie damit problemlos auf das jeweilige Benutzerkonto zugreifen – und damit auf die Daten, Systeme und das Netzwerk des Unternehmens.

VPN-CLIENTS, ANTIVIREN-/ ANTIMALWARE UND FIREWALLS SIND NICHT GENUG

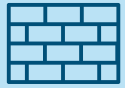
Endpoint Protection wie z. B. Client Firewalls, Malware-Schutz oder VPN-Clients sind für eine sichere IT-Umgebung, die auch remote Arbeitsplätze einschließt, Pflicht. Regelmäßige (Offline-)Backups sichern Sie zudem für den Worst-Case ab. So sind Sie schnell einsatzbereit, sollten andere Sicherheitsmaßnahmen nicht gegriffen haben. Auch eine verschlüsselte Datenübertragung sorgt dafür, dass Hacker keine relevanten Daten und Informationen abziehen können. Dennoch sichert keine dieser Maßnahmen Ihre Schwachstelle – Ihren Mitarbeiter.

SICHERN SIE IHRE USER-ACCOUNTS DURCH IAM & MFA VOR IDENTITÄTSDIEBSTÄHLEN

Ihre technischen Barrieren dürfen nicht bei Firewalls, VPN-Clients und Antivirensoftware enden. Wirkungsvolle technische Barrieren fußen insbesondere auf einem sinnvollen Identitäts- und Zugriffsrechte Management sowie einer verpflichtenden Multifaktor Authentifizierung für alle Mitarbeiter. Nur so können Sie die Identitäten sichern und vor Missbrauch schützen.

Zudem bilden die Reduzierung der von außen zugänglichen Systeme auf ein Minimum sowie eine sachgerechte interne Segmentierung der Netze eine weitere Sicherheitsstufe. Um eine tiefere Infektion Ihrer Systeme zu verhindern, sollten Sie zudem eine erhöhte Anforderung an die Passwortsicherheit mit Multifaktor Authentifizierung (MFA) an bestimmten Maschinen, Systemen oder Beriechen einführen. Ganz besonders für Administratoren und diejenigen, die über Remote-Zugangsrechte verfügen.

SOFTWARE UPDATES



FIREWALL

ANTI-VIRUS/ ANTI-MALWARE

IDENTITY & ACCESS MANAGEMENT

MULTIFAKTOR AUTHENTIFIZIERUNG

EXKURS: KRITIS-UNTERNEHMEN

Besondere Mittelständler sind die sog. KRITIS-Unternehmen. Das Funktionieren unserer Gesellschaft hängt ganz zentral an der Versorgung durch diese. Sei es unsere Energie- oder unsere Gesundheitsversorgung – ein Versagen der Infrastruktur hat Konsequenzen in allen Lebensbereichen.

Daher gilt es, diese Einrichtungen besonders zu schützen. Dies umfasst neben Präventions- und Notfallplänen an der phyischen Beschaffenheit der Einrichtungen auch immer mehr die Frage nach der Sicherheit der steuernden IT-Systeme.

Die zugrunde liegende IT ist im Zuge der Digitalisierung immer komplexer und vielschichtiger geworden: Der Einzug des (I)IoT (Industrial Internet of Things) hat Anlagen und Maschinen tief vernetzt. Selbst der punktuelle Ausfall eines Rädchens im System kann daher ungeahnte, langwierige Folgen haben.

Ein erfolgreicher Angriff hat infolge dessen ein ungemein höheres Schadpotenzial, da die Folgen über das Unternehmen hinaus auf die Gesellschaft wirken.

Daher gelten schärfere Anforderungen an (IT-)Sicherheit als für andere Unternehmen. Gleichzeitig ist die Absicherung der IT-Systeme von KRITIS-Betreibern kein leichtes Unterfangen. Zum einen handelt es sich um privat-wirtschaftliche Unternehmen verschiedener Größen. Zum anderen haben die genutzten IT-Strukturen einen langen Lebenszyklus, weshalb sie häufig nicht oder nicht zeitnah über die nötigen Sicherheitsupdates verfügen.

Trotz schärferer Anforderungen wurden bis Anfang November 2020 141 erfolgreiche Cyberangriffe gemeldet. Davon 43 auf Gesundheitsdienstleister. 2019 waren es im Bereich der kritischen Infrastruktur noch 121, 2018 sogar lediglich 62 erfolgreiche Versuche.* Neben dem Gesundheitswesen sind Energie- und Wasserversorger, Banken und Versicherungen betroffen. Meist handelt es sich bei derartigen Vorfällen um sog. Ransomware-Angriffe, die eine Lösegeldforderung zur Entschlüsselung von Daten nach sich ziehen. Aufgrund ihrer Kritikalität erhoffen sich Angreifer schnelle und hohe Lösegeldzahlungen, um eine zügige Betriebswiederaufnahme herzustellen.

*Quelle: https://www.faz.net/aktuell/wirtschaft/digitec/mehr-hacker-angriffe-auf-kliniken-und-kritische-infrastruktur-17062421.html

DOUBLECLUE – DIE LÖSUNG FÜR IHR BUSINESS

DoubleClue schützt Ihr Firmennetzwerk vor unerlaubten und schädlichen Fremdzugriffen. Die Software verbindet modernstes Identity- & Access Management (IAM) mit State of the Art Multifaktor Authentifizierung (MFA) und verfügt über weitere Security-Funktionalitäten, die den Alltag Ihrer Mitarbeiter erleichtern.

IDENTITY & ACCESS MANAGEMENT

In der übersichtlichen IAM-Plattform verwalten Sie zentral Accounts, Identitäten und Zugriffe. Das Herzstück bildet das Zugriffsmanagement auf Systeme und Anwendungen mit automatisiertem Berechtigungsmanagement und adaptiven Zugriffsrichtlinien für Applikationen und Benutzergruppen. Dies erlaubt auch die Einrichtung eines sog. Privileged Access Managements (PAM).

ZWEI-FAKTOR AUTHENTIFIZIERUNG

Die einfach umsetzbare Zwei-Faktor Authentifizierung verhindert An- und Eingriffe auf und in Ihr Netzwerk. DoubleClue bietet Ihnen alle Möglichkeiten einer modernen, passwortlosen Anmeldung: Wählen Sie aus verschiedenen Authentifizierungsmöglichkeiten die Variante, die am besten zu Ihnen passt.

SINGLE SIGN-ON (SSO)

Ihre Mitarbeiter arbeiten zeitgleich in verschiedenen Anwendungen, für die sie separate Accounts mit eigenen Zugangsdaten benötigen. Dank Single Sign-On genügt eine einzige Anmeldung im DoubleClue UserPortal, um Zugriff auf alle benötigten Applikationen zu erhalten – mit nur einem Klick.

PASSWORDSAFE MIT AUTOFILL-FUNKTION

Der DoubleClue PasswordSafe vereinfacht die Verwaltung vieler, selbst komplexer Passwörter erheblich. Speichern Sie Ihre Passwörter ganz einfach an einem Ort und greifen Sie gebündelt darauf zu – direkt aus der Webanwendung oder der mobilen App heraus. MFA und Verschlüsselung stellen sicher, dass die Passwörter in Ihrem Safe sicher verwahrt sind. Dank Autofill können Sie sich ganz bequem aus der DoubleClue App heraus überall anmelden.

DOUBLECLUE KEEPASS-PLUGIN

Dem weltweit beliebten OpenSource Passwortmanager KeePass fehlen standardmäßig zwei Dinge für die Nutzung im Unternehmensumfeld: Eine Multifaktor Authentifizierung sowie die Möglichkeit, Passwörter mit Kollegen, Partnern und Dienstleistern zu teilen. Das DoubleClue KeePass-Plugin erlaubt den einfachen Im- und Export von Passwort-(kdbx-)Dateien zwischen beiden Systemen.

DOUBLECLUE APP FÜR iOS & ANDROID

User erwarten heute eine hohe Usability. Daher bietet DoubleClue Ihnen die Möglichkeit, Passwörter und Approvals über eine moderne und übersichtliche App auf Ihrem mobilen Device zu verwalten.

DOUBLECLUE CLOUDSAFE

Wichtige und vertrauliche Dokumente sollten nie über unverschlüsselte E-Mails versendet werden. Der DoubleClue CloudSafe erlaubt Ihnen daher nicht nur die zentrale verschlüsselte Speicherung von sensiblen Daten in einem durch MFA geschützten, unzugänglichen Bereich innerhalb Ihrer eigenen IT-Infrastruktur. Er eröffnet Ihnen auch die Möglichkeit diesen Zugriff mit Ihren Mitarbeitern, Partnern oder Dienstleistern sicher zu teilen – ohne, dass Ihre Daten den Server verlassen.

Zum Produktdatenblatt

DOUBLECLUE – ANWENDUNGSFÄLLE

ABSICHERUNG VON REMOTE WORK / HOMEOFFICE

2020 war ein Katalysator für die Digitalisierung zur Zusammenarbeit in verteilten Teams. Hierzu zählen die Einrichtung von dezentralen Arbeitsplätzen in einer unsicheren Homeoffice-Umgebung sowie Neueinführung und Ausbau von digitalen Kommunikations- und Kollaborationstools (in der Cloud/ hybrid).

DoubleClue sichert die Log-ins Ihrer Mitarbeiter sowie alle Applikationen mit **Multifaktor Authentifizierung**. Über das übersichtliche **IAM-Tool** können Sie alle Zugriffsrechte zentral steuern.

Der integrierte **PasswortSafe** zur zentralen Verwaltung von Passwörtern sowie zur einmaligen Anmeldung an allen Applikationen erhöht zudem die Produktivität Ihrer Mitarbeiter dank großartiger Usability.

Im **CloudSafe** verwahren Sie Dokumente sicher an einem zentralen Ort. Den Zugriff darauf können Sie mit internen wie externen Stakeholdern teilen, sodass nicht nur Ihre Mitarbeiteridentitäten, sondern auch Ihre Firmengeheimnisse sicher sind.

ABSICHERUNG KRITISCHER INFRASTRUKTUREN

KRITIS-Unternehmen benötigen eine tiefe Absicherung Ihrer Systeme vor dem unbefugten Zugriff durch Dritte. Dies betrifft neben der Gesundheitsbranche insbesondere den Energiesektor.

GESUNDHEITSBRANCHE

Cyberattacken auf die Gesundheitsbranche haben im vergangenen Jahr stark zugenommen. Gleichzeitig schreitet die Digitalisierung zur Prozessvereinfachung bei Diagnosen und Behandlungen stark voran. Ein Hack oder Datenleak an dieser Stelle wäre jedoch fatal.

Die Gesundheitsbranche verfügt daneben über spezielle Anforderungen an die IT-Sicherheit. Oftmals sind neben Bürorechnern und Druckern auch medizinische Geräte an das Netzwerk angeschlossen. Mittels **eigener Mandanten** können verschiedene Bereiche abgetrennt werden sowie unterschiedliche Zugriffsrechte definiert werden. Server, auf denen etwa vertrauliche Patientendaten lagern, können so abgesichert werden, dass nur einzelne Personen mit besonderen Zugangsvoraussetzungen darauf Zugriff haben.

Hierfür können Sie in DoubleClue Usergruppen mit verschiedenen Kritikalitätseinstufungen anlegen. Mittels eines sog. **PAMs (Privileged Access Management)** können besonders strenge, individuelle Zugriffs- und Authentifizierungslösungen bei besonders kritischen Systemen eingesetzt werden.

Neben der verlässlichen Absicherung der (unterteilten) Netzwerke in Arztpraxen, bei Apotheken oder in Krankenhäusern, haben wir auch Lösungen für sog. Shared Access an einzelnen Maschinen entwickelt, die einen Missbrauch ausschließen und trotzdem die Arbeitsabläufe Ihrer Mitarbeiter nicht unterbrechen.

ENERGIEVERSORGER

Hier stehen besonders die Leitnetzwerke in den Bereiche Wasser-, Strom- und Gasversorgung im Zentrum. Ebenso wie die Gesundheitsbranche benötigen auch Energieversorger ein kritisches Zugriffsrecht und starke Authentifizierungslösungen. Auch hier setzen wir auf die Unterteilung der Usergruppen mittels PAM.

HWS GRUPPE

HWS INFORMATIONSSYSTEME GMBH

Die HWS Gruppe bietet ihren Kunden umfassende IT-Dienstleistungen, Softwareentwicklung und Beratungen, insbesondere in den Bereichen IT-Infrastruktur, Cloud Operations und Identity Protection. Mehr als 150 Mitarbeiter aus Neustadt an der Aisch (Mittelfranken) und dem Nearshore Delivery Center auf Malta unterstützen sowohl DAX Konzerne als auch den gehobenen Mittelstand bei ganzheitlichen IT-Projekten. Dank eines progressiven und fordernden Serviceansatzes überzeugen wir seit mehr als 20 Jahren als verlässlicher und nahbarer Partner.

IT Security made in Germany!

Unsere umfassenden IT-Security Lösung „DoubleClue" ermöglicht Unternehmen weltweit ein sicheres Identitäts- und Zugriffsmanagement sowie eine starke Multifaktor Authentifizierungslösung.

Erfahren Sie mehr über uns sowie unsere Dienstleistungen und Softwareprodukte unter **hws-gruppe.de** & **doubleclue.com**.

HWS INFORMATIONSSYSTEME GMBH
Wilhelmstr. 16 | 91413 Neustadt a. d. Aisch
+49 (0)9161 6239 200 | requests@doubleclue.com

DOUBLE CLUE
CLEVERLY SECURES IDENTITIES

Wir sind Partner

Allianz für Cyber-Sicherheit
Partner