itsecurity

DEZEMBER 2018

DAS SPEZIAL

RAPID DETECTION & RESPONSE SERVICE

PRAKTISCH GESCHÜTZT

Michael Jany, IT Administrator, Alfred Ritter GmbH & Co.KG

ERHÖHTE SICHERHEIT

Elf WAFs im Vergleich

BUSINESS-E-MAIL-COMPROMISES

„Sie haben (gefährliche) Post!"

SECURITY AWARENESS

Puzzleteil im Sicherheitskonzept

www.it-daily.net

NTT Security

Sind Sie auf dem sicheren Weg in die Cloud?

Wo auch immer Sie sich auf Ihrer Reise in die Cloud gerade befinden, wir sind stets an Ihrer Seite

Verlockende Aussichten: Kostensenkung, Zeitersparnis, weniger Komplexität – machen die Reise in die Cloud zu einem Muss. Aber kennen Sie auch die erforderlichen Sicherheitsmaßnahmen oder Best Practices für dieses All-Inclusive-Paket?

Wo auch immer Sie sich gerade auf Ihrer Cloud-Reise befinden, eines ist gewiss – wenn Sie Daten und Anwendungen in der Cloud speichern, müssen Sie überzeugt sein, dass sie sicher sind.

Bei NTT Security nehmen wir Cloud-Sicherheit sehr ernst. Unsere Experten unterstützen Sie in jeder Phase Ihres Cloud-Projektes. Gemeinsam mit Ihnen bewerten wir die Risikosituation und beherrschen alle Sicherheitsherausforderungen.

Erfahren Sie mehr über unsere Services für das Security Risk Assessment oder über unsere Managed Security Services.

Als spezialisiertes Sicherheitsunternehmen der NTT Group kombinieren wir unsere Expertise mit der von NTT Communications, NTT DATA und Dimension Data. Wir arbeiten eng zusammen, um die Komplexität zu verringern und unseren Kunden Zeit und Geld zu sparen – und zwar mit unseren maßgeschneiderten Managed Security Services.

Riskieren Sie nichts. Vertrauen Sie uns bei Ihrer Reise in die Cloud.

www.nttsecurity.com/de-de/cloud

Delivering Global Security From

NTT Communications NTT DATA dimension data

12

INHALT

PRAKTISCH

MIT RAPID DETECTION & RESPONSE SERVICE AUF DER SICHEREN SEITE.

Cyberangriffe können früher oder später jedes Unternehmen treffen. Auf der sicheren Seite ist, wer für alle Eventualitäten gut aufgestellt ist. Darüber sprach die it security-Redakteurin Carina Mitzschke mit Michael Jany, IT Administrator bei Ritter Sport.

Carina Mitzschke: *Herr Jany, im Juni 2017 hatte ein anderer Schokoladenhersteller einen Produktionsausfall aufgrund eines Hackerangriffes. Wie sahen Ihre eigenen Security-Maßnahmen zu diesem Zeitpunkt aus?*

Michael Jany: Wir haben den Fall natürlich über die Medien verfolgt. Unser Hauptsitz und einziger Produktionsstandort befindet sich in Waldenbuch. Ein durch Hacker verursachter Stillstand unserer Produktion hätte entsprechend fatale Auswirkungen auf die weiteren Geschäftsprozesse und wäre uns teuer zu stehen gekommen. Deshalb haben wir unsere eigenen Sicherheitsmaßnahmen auf den Prüfstand gestellt. Zu diesem Zeitpunkt war unsere Infrastruktur nicht besser oder schlechter geschützt als die der meisten anderen Unternehmen, mit einem mehrstufigen AV-Scan für eingehende E-Mails, sowie AV-Scan auf Clients und Servern.

Carina Mitzschke: *Die meisten Unternehmen sprechen nicht darüber, dass sie angegriffen wurden. Sie gehen damit sehr offen um – warum?*

Michael Jany: Vermutlich sprechen sie nicht darüber, weil sie nicht wissen, dass sie angegriffen worden sind oder sie möchten sich nicht die Blöße geben. Aber Spaß beiseite, es ist wichtig über Cyberkriminalität zu sprechen und für das Thema ein Bewusstsein zu schaffen – und das nicht nur in den Fachmedien.

Dennoch würden auch wir einen zielgerichteten Angriff nicht in die Öffentlichkeit tragen, sondern uns intern mit der Sache auseinander setzen. Glücklicherweise waren wir noch nicht in der Situation, sind aber für alle Eventualitäten gerüstet.

> ES IST WICHTIG ÜBER CYBERKRIMINALITÄT ZU SPRECHEN UND FÜR DAS THEMA EIN BEWUSSTSEIN ZU SCHAFFEN – NICHT NUR IN DEN FACHMEDIEN.
>
> Michael Jany, IT Administrator, Alfred Ritter GmbH & Co.KG

Carina Mitzschke: : *Welche Art von Cyberattacken trifft Ritter Sport am häufigsten? Malware, DDoS-Attacken oder eher Ransomware?*

Michael Jany: Am häufigsten sind wir tatsächlich mit opportunistischen Attacken konfrontiert. Also Attacken, die nicht uns direkt adressieren und versuchen per Gießkanne so viel Opfer wie möglich zu erreichen. In unserem Fall nutzen die Angreifer E-Mails und setzen Malware sowie Ransomware ein.

Wichtig dabei ist aber auch zu erwähnen, dass viele E-Mails durch die AV nicht als schadhaft eingestuft werden und entsprechend in den Posteingängen der Mitarbeiter landen. Deswegen schulen wir unsere Mitarbeiter regelmäßig, wie sie die „guten" von den „bösen" E-Mails unterscheiden können. Und wenn dann doch mal auf einen Link in der „bösen" E-Mail geklickt oder ein Makro im Word-Dokument aktiviert wird, dann greifen immer noch andere Maßnahmen.

GESCHÜTZT

Carina Mitzschke: *Das Rapid Detection & Response System (RDS) von F-Secure ist so eine Maßnahme, oder? Können Sie kurz erläutern, warum Sie sich für die Lösung entschieden haben?*

Michael Jany: Das ist korrekt. Im Bereich der Endpoint Protection haben wir die F-Secure Business Suite Premium im Einsatz, mit der wir bereits gute Erfahrungen gemacht hatten. In RDS sehen wir nun die perfekte Ergänzung zu unserem ganzheitlichen Sicherheitskonzept, das nun auch den Bereich „Erkennen und Reagieren" abdeckt. Eben auch für den Fall, das doch mal eine „böse" E-Mail durchrutschen sollte. Aber auch darüber hinaus. Wir haben RDS jetzt schon seit einiger Zeit im Einsatz und haben einen großen Gewinn an Sicherheit durch die Sicherheitsmechanismen erzielt. Dass die Entscheidung die Richtige war, beruht nicht zuletzt auf der Tatsache, dass in letzter Instanz immer der Mensch über die Meldungen schaut und eine fundierte Entscheidung trifft.

Carina Mitzschke: *Was ist der Vorteil der F-Secure gegenüber anderen marktgängigen Lösungen? Wie funktioniert die Lösung?*

Michael Jany: Zunächst war es uns wichtig, einen europäischen Hersteller und deutschen Partner mit strikter „No-Backdoor"-Politik zu wählen und den haben wir mit F-Secure gefunden. Am meisten hat uns aber die Tatsache überzeugt, dass die Handhabung sehr einfach vonstattenging. Bis auf die Verteilung der Agents erforderte es keine weiteren Aktionen bei der Implementierung von unserer Seite.

Ein weiterer Vorteil war, dass die Lösung gleich nach der Implementierung auch eingesetzt werden konnte. Kein mühseliges Anlernen der Algorithmen, keine Schulung der Mitarbeiter. Die Lösung ist so konzipiert, dass die dazu gehörige KI anomales Verhalten auf Rechnern und im Netzwerk aufspürt, analysiert und im Ernstfall durch die Threat Hunting Experten von F-Secure evaluiert und Hackeraktivitäten meldet.

Carina Mitzschke: *Eine Implementierung von neuen Lösungen kostet immer Zeit und auch Budget. Wie gestaltete sich hier der Ablauf?*

Michael Jany: Der Zeitaufwand hat sich auf das Verteilen der Agents beschränkt und war somit erfreulich gering. Wir überwachen jeden Client und Server.

Carina Mitzschke: *Apropos Ernstfall: Wie schnell schlägt der Rapid Detection & Response Service von F-Secure an und wie sieht die Reaktion aus?*

Michael Jany: F-Secure hat sich vertraglich auf eine Reaktionszeit von maximal 30 Minuten verpflichtet. Die Realität hat uns aber gezeigt, dass das eher das oberste Maximum ist und wir überwiegend Meldezeiten von unter 10 Minuten haben.

Die Reaktion sieht dabei so aus, dass wir von F-Secure einen Anruf bekommen. Ein Codewort legitimiert den Anrufer und es werden weitere Schritte besprochen beziehungsweise Handlungsempfehlungen, wie man vorzugehen hat, um weiteren Schaden abzuwenden. RDS steht 24/7 zur Verfügung. Das heißt, es könnte auch schon mal vorkommen, dass ein Anruf mitten in der Nacht erfolgt. Das ist dann zwar nicht so förderlich für meinen Schlaf, aber Cyberkriminalität schläft nicht und da zählt jede Sekunde.

Carina Mitzschke: *Haben Sie je ein professionelles Hackerteam engagiert, um die Lösung oder generell Ihre Abwehr zu testen? Wenn ja, wie weit sind sie gekommen?*

Michael Jany: Natürlich wollten wir herausfinden, wie die Erkennung und Reaktion bei F-Secure abläuft und haben daher mit einem externen Partner ein Red Team auf einem Client durchgeführt. Weit sind sie nicht gekommen. Nach nicht einmal 5 Minuten hat F-Secure den Angriff gemeldet, weitere Maßnahmen eingeleitet und somit Schaden abgewendet.

Carina Mitzschke: *Thema DSGVO: Hosten Sie Ihre Daten selber oder sind sie in eine Cloud ausgelagert?*

Michael Jany: Nachdem wir eben nur diesen einen Produktionsstandort haben, sind wir in der glücklichen Situation, die Daten nicht in der Cloud lagern zu müssen. Daher hosten wir unsere Daten selber.

Carina Mitzschke: *Herr Jany, wir danken für dieses Gespräch.*

SCHOKOLADE MIT SICHERHEIT

ÜBERWACHEN – ANALYSIEREN – BEWERTEN.

Schon 20 Jahre nach Firmengründung gelingt der Alfred Ritter GmbH & Co.KG 1932, mit der Erfindung des Schokoladenquadrates, eine wegweisende Einführung, die bis heute eine der prägendsten Schokoladenmarken ist.

Modern wie die heutigen Produktionsmaschinen ist auch die IT, auf die sich mehr als 1400 Mitarbeiter weltweit verlassen. Spektakuläre Cyberangriffe, die 2016 und 2017 international unzählige Betriebe lahmlegten, haben das Unternehmen überzeugt, dass es ein Frühwarnsystem benötigt, um diese wirksam abzuwehren.

Die perfekte Cyber-Abwehr

Pro Tag werden rund 3 Millionen Tafeln Ritter Sport Schokolade am Produktionsstandort Waldenbuch hergestellt. Ein durch Hacker verursachter Stillstand der Produktion hätte fatale Auswirkungen auf die weiteren Geschäftsprozesse und könnte dem Fabrikanten teuer zu stehen kommen. Das hat bereits ein anderer Schokoladenhersteller zu spüren bekommen, dessen Produktion durch einen Petya-Angriff im Juni letzten Jahres eine Woche lang stillstand.

Auch ein noch so guter Schutz gegen Computerviren und Malware ist vielfach machtlos, wenn es um Cyberattacken in Form von Ransomware („Erpressertrojanern") oder gar zielgerichteten Attacken geht. Meist nutzen die Angreifer dabei die Schwachstelle Mensch aus. Mit Spear-Phishing-Methoden werden ahnungslose Mitarbeiter zum Ausführen einer Aktion wie beispielsweise einem Klick auf eine URL oder dem Aktivieren von Makros in Dokumenten verleitet. In Folge dessen nistet sich der Angreifer unbemerkt ins Unternehmensnetzwerk ein und beginnt, Daten abzugreifen oder wie im Petya-Fall eine Ransomware auszurollen und Systeme im Netz zu verschlüsseln.

Für Ritter war das der Anlass, umgehend ein Warnsystem einzurichten, das verdächtiges Verhalten im Unternehmensnetz registriert. Die Wahl fiel dabei auf F-Secure Rapid Detection & Response Service (RDS) mit Managed Detection and Response Service, zumal der Schokoladenhersteller nach erfolgreicher Einführung der Business Suite Premium zum Schutz der PC-Systeme und vielen eingesetzten Citrix-Terminalserver bereits gute Erfahrungen mit dem finnischen Anbieter gemacht hat.

Und RDS kam gerade rechtzeitig: Bei einem gezielten Angriff auf die Finanzbuchhaltung von Ritter im November 2017 meldete das F-Secure Team den entsprechenden Vorfall in nur 9 Minuten - und war damit deutlich schneller als die von F-Secure regulär versprochene Reaktionszeit von maximal 30 Minuten.

Ein anderer Vorfall im März 2018 wurde von F-Secure Rapid Detection & Response Service sogar innerhalb von nur 6 Minuten gemeldet. Auch hier stand einmal mehr Microsoft Office im Mittelpunkt und ein bösartiges Makro löste ein ungewöhnliches Verhalten im System aus. Auch diese Informationen wurden von den Sensoren gesammelt, die nachgeschalteten Incident Analysten erkannten die Spur eines Angriffes und der Vorfall sofort gemeldet werden.

Beide Angriffe basierten auf dem Angriffsvektor E-Mail. Und das ist auch nicht unüblich, wie der jüngste Incident Response Bericht von F-Secure zeigt. Laut dem Report starten mehr als ein Drittel aller digitalen Zwischenfälle mit einer Phishing-E-Mail oder einem bösartigen Anhang, der an Mitarbeiter verschickt wird. Die häufigste Schwachstelle, die dabei ausgenutzt wird, sind Lücken in Softwareangeboten, die vom Internet aus zugänglich sind. In 21 Prozent der von F-Secure untersuchten Fälle konnten Angreifer solche Schwachstellen nutzen, um in die Firmeninfrastruktur einzudringen.

In 34 Prozent aller Fälle war allerdings keine Lücke notwendig, hier erfolgte der Angriff über Phishing und bösartige Anhänge in E-Mails. Angriffe, die für Unternehmen viel schwerer in den Griff zu bekommen sind.

Warum RDS?

Jeden Tag analysiert das F-Secure Labor hundert Tausende Malware Samples, die für nicht zielgerichtete Angriffe verwendet werden und mit einem zuverlässigen Endpoint-Schutz gestoppt werden können. Doch die Zahl der Cyber-Attacken, die herkömmliche Schutzmechanismen durch eigens entwickelte Malware und Exploits raffiniert umgehen, ist sprunghaft angestiegen. Zur Abwehr gezielter Hacker-Attacken und Datendiebstahls im großen Stil stehen CIOs und CISOs heute vor der Herausforderung, ihre komplexen IT-Systeme umfassend zu überwachen, Angriffe sofort zu erkennen und die entsprechenden Gegenmaßnahmen einzuleiten. Dabei helfen nur neue Abwehrmaßnahmen wie Managed Detection & Response sowie Incident Response Services, die F-Secure mit RDS abdeckt.

Für die schnelle Erkennung von Cyberangriffen setzt die Komplettlösung RDS auf eine Künstliche Intelligenz und zusätzlich auf ein Team internationaler Threat Hunting Experten. Dieses entscheidet bei jedem Vorfall, ob er eskaliert und gemeldet werden soll oder nicht. Denn wie eine andere F-Secure-Studie zeigt, erweisen sich 13 Prozent aller untersuchten Vorkommnisse, zu denen F-Secure im Rahmen einer Incident Response Untersuchung in Unternehmen gerufen wurde, als falscher Alarm. Die Sicherheitsverantwortlichen bei Ritter oder auch andere Unternehmenskunden werden anschließend nicht per E-Mail oder SMS auf den akuten Fall hingewiesen, sondern ausschließlich telefonisch. Hierfür ist das F-Secure Threat Hunting Team im 24/7/365-Betrieb im Einsatz, um Angriffe zu überwachen, zu analysieren und zu bewerten - um dann im richtigen Moment zu reagieren.

Zuverlässiger Schutz mit zuverlässigen Partnern

Wie bereits beim ersten Projekt zwischen Ritter und F-Secure, der Implementierung der Business Suite Premium, hat auch die Einführung des RDS-Frühwarnsystems wieder die BWG Informationssysteme GmbH betreut. Wie Ritter System Administrator Michael Jany betont, war es dem Unternehmen in beiden Fällen wichtig, einen europäischen Hersteller und deutschen Partner mit strikter „No-Backdoor"-Politik zu wählen.

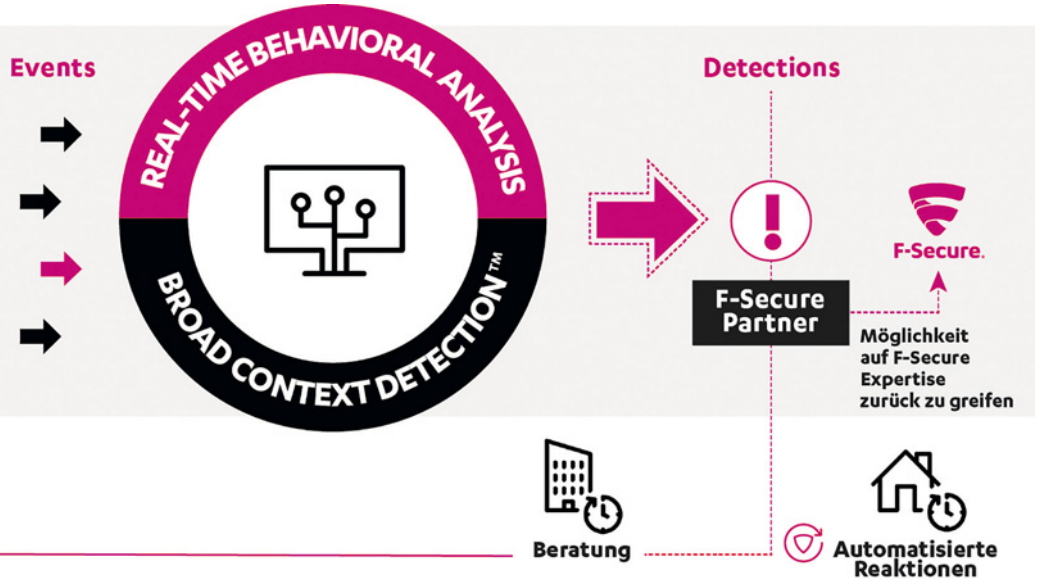
Rapid Detection Service umfasst die 24/7-Überwachung durch F-Secure für die rund 1.000 angeschlossenen Server-Endpoints bei Alfred Ritter. Das F-Secure-Versprechen, in maximal 30 Minuten einen Sicherheitsvorfall zu erkennen und zu melden, konnte bei beiden Angriffen deutlich unterschritten werden. Damit stellt sich auch ein sofortiger Return on Invest (ROI) ein. „Das hat nicht nur uns IT-Verantwortliche, sondern auch den Finanzchef und die Controller überzeugt", sagt Jany.

„Mit der Business Suite Premium und dem Rapid Detection & Response Service von F-Secure sind unsere Systeme nun rundum gegen alle Formen von Malware und Cyberattacken geschützt.

Die beiden Fälle, die RDS bei uns seit der Einführung in so kurzer Zeit aufgedeckt hat, haben uns mehr als überzeugt, uns für die richtige Lösung entschieden zu haben. Mehr noch, wir sehen F-Secure mit seinen Experten aus dem Rapid Detection Center als vollwertige Mitglieder unseres Sicherheitsteam.", so Michael Jany.

www.f-secure.com/de

F-SECURE RAPID DETECTION & RESPONSE



1. Ressourcenschonende Sensoren überwachen Endgeräteaktivitäten, die von Angreifern ausgelöst wurden, und streamen Ereignis- und Verhaltensdaten in Echtzeit in die F-Secure Cloud.
2. Die Datenanalyse und „Broad Context Detection" -Verfahren grenzen die Daten ein und identifizieren rasch echte Angriffe.
3. Nach einer bestätigten Erkennung führt die F-Secure RDR-Lösung durch die Schritte, mit denen Sie die Bedrohung eindämmen und beheben.

SECURITY

> ES GILT, DAS UNTERNEHMEN CYBERSICHER ZU MACHEN, OHNE DIE EFFIZIENZ VON GESCHÄFTSPROZESSEN ZU BEEINTRÄCHTIGEN.
>
> Alexander von Keller, Head of Corporate Sales DACH bei Kaspersky Lab www.kaspersky.de/awareness

Cyberattacken zielen oft auf Mitarbeiter ab. Umso wichtiger ist es, dass diese die Gefahr frühzeitig erkennen, richtig darauf reagieren und sicheres Verhalten im Arbeitsalltag verinnerlichen. Doch wie lässt sich Security Awareness im Unternehmen aufbauen? Darüber sprach it security mit Alexander von Keller, Head of Corporate Sales DACH bei Kaspersky Lab.

it security: *Herr von Keller, wie groß ist die Cybergefahr für Unternehmen?*

Alexander von Keller: Sie wächst ständig. Unternehmen jeder Größe sind mit einem zunehmenden Aufkommen an Cyberbedrohungen konfrontiert. So entdeckten unsere Systeme 2017 jeden Tag durchschnittlich 360.000 schädliche Dateien. Das sind fast 12 Prozent mehr als im Vorjahr. Wir haben diese Malware-Kennzahl erstmalig 2011 berechnet – mit damals nur etwa 70.000 neuen Varianten pro Tag. Die Menge an verbreiteter Schadsoftware hat sich also innerhalb nur weniger Jahre um das Fünffache erhöht. Und wenn ein Unternehmen unvorbereitet von Cyberkriminellen angegriffen wird, kann das richtig teuer werden. Durchschnittlich 83.000 US-Dollar finanzieller Schaden entsteht bei kleinen und mittelständischen Unternehmen allein durch unvorsichtiges Verhalten oder Unwissenheit von Mitarbeitern im Zusammenhang mit einem Sicherheitsvorfall.

it security: Also müssten Mitarbeiter im Bereich IT Security besser geschult werden?

Alexander von Keller: Ja, absolut. Die Mitarbeiter selbst sind nämlich eine ernstzunehmende Sicherheitslücke im Unternehmen. Das belegen auch unsere Studien: So waren 2016 rund 46 Prozent der Cybersicherheitsvorfälle auf unachtsame Angestellte zurückzuführen. Eine andere Kaspersky-Umfrage fand heraus, dass lediglich 12 Prozent der Mitarbeiter sich über Regeln zur IT-Sicherheit in ihren Unternehmen vollkommen bewusst sind. Dies zeigt, dass hier dringender Handlungsbedarf besteht. Mitarbeiter sind ein unverzichtbares Puzzleteil im großen Cybersecurity-Konzept eines Unternehmens. Sie nehmen für Cyberkriminelle eine Schlüsselfunktion ein, die das Einschleusen von Malware ins Unternehmen oft erst möglich macht. Deshalb ist es notwendig, dass jeder einzelne über vorherrschende Compliance-Vorgaben sowie gängige Taktiken von Cyberkriminellen Bescheid weiß, Indikatoren für einen möglicherweise laufenden Angriff bemerkt und entsprechend richtig darauf reagiert. Dies alles lässt sich in Schulungen vermitteln. Grundsätzlich gilt: Je mehr Mitarbeiter ein Bewusstsein für Security aufbauen, umso besser ist es für die gesamte Unternehmenssicherheit.

it security: *Worauf kommt es bei Schulungsmaßnahmen an?*

Alexander von Keller: Das Problem bei traditionellem Frontalunterricht ist oft, dass er zu „trocken" aufbereitet ist. Folglich stoßen die übermittelten Inhalte nicht auf das nötige Interesse, verankern sich nicht im Kopf der Mitarbeiter und werden in der Konsequenz im Unternehmensalltag auch nicht gelebt. Wir haben deshalb einen anderen Ansatz gewählt, um Schulungsteilnehmern das Thema IT Security nahezubringen. Im Vordergrund stehen bei uns das interaktive Lernen und die persönliche Erfahrung im Umgang mit Cyberkriminalität. Wir haben auf dieser Basis unterschiedliche Schulungsangebote entwickelt, so dass wir Unternehmen die jeweils passende Lösung für ihre Weiterbildungsanforderungen zur Verfügung stellen können. Die Inhalte sind auf bestimmte Zielgruppen ausgerichtet und unterstützen einen langfristigen Aufbau von Security Awareness – in verschiedenen Branchen wie auch auf unterschiedlichen Unternehmensebenen.

it security: *Könnten Sie näher erläutern, welche Zielgruppen Sie ansprechen?*

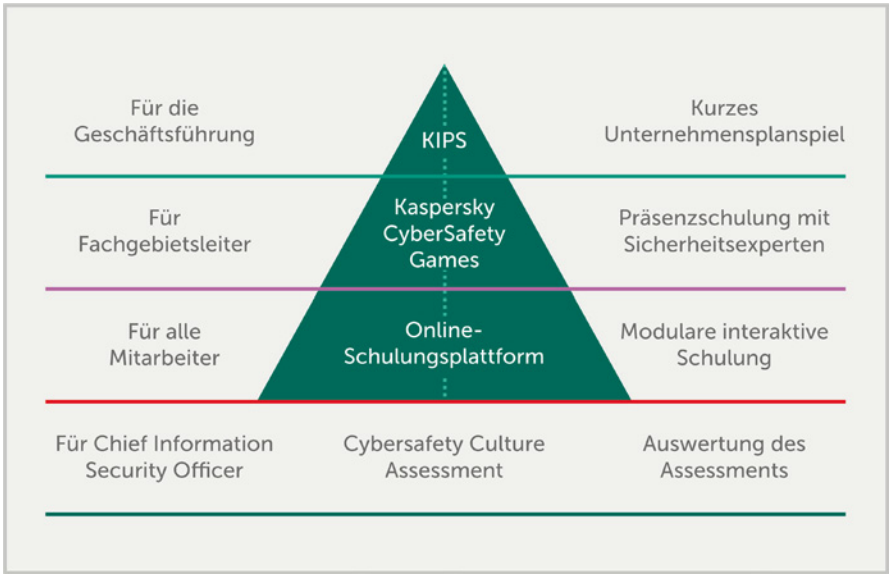
Alexander von Keller: Zu den klassischen Cyberangriffszielen zählen bekanntermaßen die Endgeräte der Mitarbeiter. Von hier aus ist es leicht, ins IT-Netzwerk vorzudringen. In manchen Fällen ist dafür nur eine E-Mail nötig. Phishing-Mails, Ransomware-Anhänge oder enthaltene Links auf gefälschte URL-Adressen nutzen stets das fehlende Know-how ihrer Opfer im Be-

AWARENESS

„MITARBEITER SIND EIN UNVERZICHTBARES PUZZLETEIL IM CYBERSECURITY-KONZEPT."

reich Cybersicherheit aus. Genau an dieser Stelle setzen unsere Online-Training-Plattform und unsere Lösung Automated Security Awareness Platform an. Sie richten sich an Mitarbeiter aller Abteilungen.

Adressieren also auch diejenigen, die bisher mit dem Thema IT-Sicherheit kaum oder gar nicht in Kontakt gekommen sind, durch ihre Arbeit am PC und mit dem Internet aber potenzielle Einfallstore für Cyberattacken darstellen. Die Schulungseinheiten mit ganz praktischen Übungen und der Wirklichkeit entnommenen Szenarien machen Mitarbeitern die Risiken bewusst, die im Arbeitsalltag auftreten können. Insgesamt sind dafür mehr als 25 interaktive Lernmodule enthalten, die alle Bereiche der Sicherheit abdecken – vom Datenschutz über simulierte Phishing-Angriffe und E-Mail-Sicherheit bis hin zum Umgang mit Passwörtern. Durch das praxisnahe Training können Mitarbeiter in der realen Welt potenzielle Bedrohungen besser erkennen und wissen, wie sie im Ernstfall richtig darauf reagieren sollen.



Kaspersky Security Awareness

? it security: *Was zeichnet die Online-Trainingsplattformen noch aus?*

Alexander von Keller: Sie bringen die typische Flexibilität von Online-Schulungen mit sich: Die Mitarbeiter lernen im eigenen Tempo direkt an ihren Computern und können sich selbst ihre Schulungszeit im Laufe des Arbeitstages einteilen. So schärfen die Trainings auf spielerische, aber trotzdem sehr einprägsame Weise das Bewusstsein für Sicherheitsgefahren. Eine Besonderheit ist auch das automatisierte Management, das beispielsweise Mitarbeitern je nach Wissensstand bestimmte Lerninhalte zuweist. Unternehmen haben also keinen Verwaltungsaufwand mit der Lösung. Außerdem gibt es viele Reporting-Funktionen, um Fortschritte einzelner Mitarbeiter oder aller Anwender kontinuierlich zu überprüfen und so Erfolge für das unternehmensweite Cybersecurity-Konzept messen zu können.

? it security: *Gibt es auch ein Angebot für die Management-Ebene?*

Alexander von Keller: Ja, denn hier sind andere Kompetenzen hinsichtlich Security Awareness gefragt. Unsere Schulungslösung für das Management nennt sich CyberSafety Management Games. Dies sind interaktive Vor-Ort-Workshops, die Führungskräften vermitteln, wie sie Compliance-konformes Verhalten unter Mitarbeitern durchsetzen und eine sichere Arbeitsumgebung in ihren Abteilungen schaffen können. Es gilt, das Unternehmen cybersicher zu machen, ohne die Effizienz von Geschäftsprozessen zu beeinträchtigen. Ganz nach dem Motto „Learning by doing" sammeln Führungskräfte Erfahrungen, um in Zukunft verantwortungsvolle und fundierte Entscheidungen bei realen Sicherheitsvorfällen treffen zu können.

? it security: *Sie sprachen auch die Branchen an ...*

Alexander von Keller: Jede Branche hat andere „wunde Punkte", die von Cyberkriminellen angegriffen werden können. Deshalb steht unser drittes Schulungsangebot, das Strategie-Simulationsspiel Kaspersky Interactive Protection Simulation (KIPS), in verschiedenen Szenarien zur Verfügung: für Unternehmen allgemein sowie für Banken, E-Government und Industrie. Geschäftsführer und Entscheidungsträger lernen hier, was es in puncto Cybersicherheit zu beachten gilt. Das Training versetzt die Teilnehmer in eine simulierte Geschäftsumgebung, in der sie einer Reihe unerwarteter Cyberbedrohungen ausgesetzt sind. Die Idee besteht darin, durch vorausschauende und schnelle Reaktionen in Teamarbeit eine Cyberverteidigungsstrategie zu entwickeln, die auch betriebswirtschaftliche Konsequenzen wie Geschäftskontinuität, Verluste oder Reputationsbeeinträchtigungen berücksichtigt.

! it security: *Herr von Keller, wir danken für dieses Gespräch.*

CLOUD NATIVE

KORIS KUBERNETES-DISTRIBUTION FÜR DIE FINANZBRANCHE.

Innovationen von FinTech-Start-ups setzen Banken und Finanzdienstleister mächtig unter Druck. Immer deutlicher wird, wie entscheidend moderne IT-Infrastrukturen für den wirtschaftlichen Erfolg in diesem Wirtschaftszweig sind.

Cloud-Native-Architekturen versprechen hohe Betriebsstabilität, Geschwindigkeit und Flexibilität. Doch der Weg dorthin ist steil: Es fehlt an Kapazitäten und an Kompetenzen – insbesondere im Bereich von Kubernetes und Containerisierung, dem Herzstück von Cloud-Native-Architekturen. Jetzt ergreift noris network die Initiative: Als bundesweit erster IT-Dienstleister bietet noris network mit KORIS eine auf die Anforderungen der Finanzindustrie zugeschnittene Kubernetes-Distribution. Ergänzend hierzu machen Betriebs- und Beratungsleistungen KORIS zu einem besonders attraktiven Lösungspaket für die Finanzbranche. So betreiben IT-Experten Kubernetes-Cluster als Managed Services auf Wunsch sowohl auf den noris network-eigenen Cloud-Plattformen als auch auf dedizierten Clustern in den noris network-eigenen nach Bankenstandards zertifizierten Hochsicherheitszentren. IT-Teams der Kunden werden im Betrieb der Cloud-Native-Anwendungen, der Test- und Deployment-Automatisierung oder der Anbindung klassischer IT-Systeme durch DevOps-Teams unterstützt.

> KORIS GIBT ENTWICKLERN DER FINANZINDUSTRIE EINE LÖSUNG AN DIE HAND, DIE ÜBLICHE HERAUSFORDERUNGEN WIE NACHWEISBARER RECHTSKONFORMER BETRIEB, NETZWERKSICHERHEIT ODER ARCHIVIERUNG OUT-OF-THE-BOX BEANTWORTET.
>
> Jürgen Städing, Vorstand, noris network AG | www.noris.de

Kubernetes für die Finanzbranche & Steuerberater

Die Zukunft liegt auch für die Finanzbranche in der Cloud. Doch „die Cloud" im Allgemeinen zeigt sich nicht immer vorbereitet auf die speziellen Anforderungen von Unternehmen wie Banken, Versicherungen und anderer Finanzdienstleister. Das bedeutet, dass auch in der Cloud individuelle Lösungen gefunden werden müssen, um den Ansprüchen dieser Branche gerecht zu werden.

Die nächste Hürde: Anwendungen benötigen Daten, die in den klassischen, oft proprietären IT-Systemen der Finanzinstitute vorgehalten werden. Es müssen also hybride Infrastrukturen entworfen, aufgebaut und betrieben werden. Die meisten IT-Verantwortlichen in der Branche sehen den Bedarf, können aber den gordischen Knoten aus erforderlichen Kompetenzen, Ressourcen, Tools, hybrider Infrastruktur, Erfahrungen, Sicherheitsanforderungen, Zertifizierungen, Kapazitäten und vielem mehr nicht durchschlagen.

Vorsprung geben

In diese Lücke stößt noris network jetzt mit KORIS. Die Cloud-Spezialisten bieten mit dieser spezialisierten Kubernetes-Distribution eine Entwicklungs- und Betriebsplattform für moderne finanztechnologische Lösungen. „Wir sind als Betreiber von Hochsicherheitsrechenzentren sowie als Infrastruktur und Managed Service Provider seit Jahrzehnten Partner der Finanz- und Versicherungsbranche. Wir beobachten täglich, wie groß der Aufwand ist, klassische IT in flexible und skalierbare Cloud-Lösungen zu überführen und dabei die besonderen Sicherheits- und Datenschutzanforderungen der Branche einzuhalten", erläutert Jürgen Städing, Vorstand bei der noris network AG.

„Mit KORIS haben wir eine spezialisierte Kubernetes-Distribution zusammengestellt, die diese Fragestellungen adressiert und Kubernetes mit den notwendigen Modulen bereitstellt, um den Anforderungen im Finanzbereich aber auch von Berufsständen wie Rechtsanwälten und Wirtschaftsprüfern gerecht zu werden.

Diese Plattform gibt Entwicklern der Finanzindustrie eine Lösung an die Hand, die übliche Herausforderungen wie nachweisbarer rechtskonformer Betrieb, Netzwerksicherheit oder Archivierung out of the box beantwortet. Sie können sofort auf einer hochskalierbaren Plattform aufsetzen, die sowohl in eine hybride Infrastruktur nahtlos integriert, als auch von unserer jahrzehntelangen Erfahrung in der Finanzbranche profitiert."

CYBERCRIME

DER BEDROHUNGSLAGE EFFEKTIV BEGEGNEN.

UNSERE KUNDEN SIND NACH DER EINFÜHRUNG VON CISCO UMBREALLA REGELRECHT ERSTAUNT, WIE VIELE BEDROHUNGSSZENARIEN AUTOMATISCH VON DEM SYSTEM GEBLOCKT WERDEN. HÄUFIG IST DEN SECURITY-VERANTWORTLICHEN VORHER GAR NICHT BEWUSST, WIE VIELE ANGRIFFE TÄGLICH PASSIEREN.

Stefan Mulder, Client Solution Director Cyber Security, Logicalis GmbH
www.logicalis.de

Intensität und Einfallsreichtum von Cyberangriffen nehmen weiter zu. Für einen wirksamen Schutz benötigen Unternehmen zwei Dinge: Effektive Security-Lösungen zur Abwehr der komplexen Bedrohungen und das notwendige Know-how, um diese Technologien zu beherrschen – bei Bedarf mit der Hilfe von externen Experten.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) legt es in seinem Lagebericht zur IT-Sicherheit 2018 zweifelsfrei dar: Die Gefährdungslage durch Cyberkriminalität nimmt keinesfalls ab; ganz im Gegenteil: Sie hat sich weiter verschärft und ist vielschichtiger geworden. Dabei existiert nach wie vor eine hohe Dynamik der Angreifer bei der Weiterentwicklung von Schadprogrammen und Angriffswegen. Für Unternehmen bedeutet dies, dass es immer anspruchsvoller wird, ihre IT-Infrastruktur wirkungsvoll abzusichern.

Fachkräftemangel verschärft Brisanz

Diese Herausforderung gewinnt an doppelter Brisanz, berücksichtigt man den aktuellen Fachkräftemangel im IT-Bereich. Laut einer repräsentativen Umfrage von Bitkom Research gab es bereits im September vergangenen Jahres 55.000 offene Stellen für IT-Experten; IT-Sicherheitsexperten sind hierbei gefragter denn je. Sie liefern das notwendige Know-how, um die modernen, teils sehr komplexen IT-Sicherheitslösungen implementieren und beherrschen zu können.

Cloudbasierte IT-Security-Lösungen

Unternehmen, die sich schnell und umfassend gegen neuartige Cyberangriffe wie beispielsweise Cryptomining rüsten wollen, können auf Cloudbasierte IT-Security-Lösungen wie Cisco Umbrella zurückgreifen. Sie blockiert als erste Verteidigungslinie auf der DNS-Ebene potenziell gefährliche Anfragen, noch bevor die Verbindung hergestellt wird. Damit schützt sie Unternehmen und deren mobile Mitarbeiter vor Bedrohungen innerhalb und außerhalb des eigenen Unternehmensnetzwerkes. Ein Vorteil ist die schnelle Implementierbarkeit: Das Secure-Internet-Gateway spannt seinen „Schutzschirm" binnen Minuten über sämtliche Nutzer und integriert sich in bestehende Systeme.

Klingt einfach, ist es für viele Unternehmen in letzter Konsequenz aber nicht. Wenn es darum geht, moderne IT-Sicherheitslösungen wie Cisco Umbrella zu implementieren und auch wirklich effektiv zu betreiben, scheitern viele Unternehmen an Budgetvorgaben und/oder fehlender interner Expertise. Oft schöpfen sie deshalb das Potenzial der Security-Lösungen nicht aus. An dieser Stelle helfen externe Experten. Logicalis bietet mit Managed Umbrella Response zum Beispiel eine Managed-Service-Leistung, die den Einsatz von Cisco Umbrella für die Abwehr von Internet-Bedrohungen optimiert und konkrete Handlungsempfehlungen ableitet.

Externe Unterstützung erspart Investitionen

Als Managed Service Provider implementiert und verwaltet Logicalis bei Bedarf auch ganzheitliche IT-Sicherheitskonzepte: Diese umfassen unter anderem Präventionsmaßnahmen zur Früherkennung von Angriffen, die Absicherung der Infrastruktur mit Firewalls oder auch Endpoint-Protection zum Schutz von PCs und anderen Geräten. Logicalis verfügt hierfür über ein spezialisiertes Security Operation Center, in dem die notwendige Expertise sowie die benötigte Palette an Lösungen und Services konzentriert vorhanden sind. Das erspart Kunden eigene Investitionen in diesem Bereich und hilft bei einem effektiven Rundum-Schutz.

Stefan Mulder

LOGICALIS
Business and technology working as one