Technology Dossier

Workplace-Transformation

IT-Security für den mobilen Arbeitsplatz: Überall sicher arbeiten

Informationssicherheit ist keine Frage des Arbeitsortes, sie ist Grundlage jeder Unternehmenstätigkeit. Das erfordert neue Sicherheitskonzepte, Strategien und Lösungen.

IDG

In Kooperation mit CIO hp

Excecutive Summary

Die Pandemie hat die Entwicklung hin zu Remote Work beschleunigt. Künftig werden Mitarbeiter gleichermaßen im Büro und im Home-Office tätig sein, damit wird sich Hybrid Work etablieren.

Doch gezielte Attacken auf Nutzer und Systeme im Home-Office zeigen: Die IT-Sicherheit an den neuen Arbeitsorten muss auf das gleiche, hohe Niveau wie innerhalb des Unternehmens gebracht werden.

Bislang wurden Security-Maßnahmen zentral organisiert. Das reicht nicht mehr aus. Stattdessen muss die IT-Sicherheit direkt an jedem beliebigen Ort wirksam sein, an dem gearbeitet wird.

Dafür sind Konzepte und Lösungen gefragt, die direkt auf den Endgeräten Risiken erkennen und abwehren. Ebenso müssen die Nutzer als Teil der Security verstanden und für ein sicheres Verhalten am digitalen Arbeitsplatz sensibilisiert werden

.

Inhalt

Die neue Realität: Home-Office als Regel, nicht als Ausnahme

Die Konzepte für IT-Sicherheit müssen an die neue Realität des Arbeitens angepasst werden. Temporäre Lösungen, um Tätigkeiten im Home-Office abzusichern, haben ausgedient. Die Endpoint-Sicherheit muss neu gedacht werden, vom Endgerät und von der Nutzerin und dem Nutzer aus.

Die große Mehrheit der Unternehmen hat seine Beschäftigten wegen Corona ins Homeoffice geschickt, berichtet der Digitalverband Bitkom. Gut jedes dritte Unternehmen (37 Prozent) hat erst in der Pandemie Home-Office eingeführt.

Weitere 44 Prozent haben Regelungen ausgeweitet, die bereits zuvor bestanden. Insgesamt ermöglichten im November 2021 acht von zehn Unternehmen (81 Prozent) ihren Beschäftigten, auch außerhalb der Betriebsstätte zu arbeiten.

Zu Beginn der Pandemie fand der Wechsel ins Home-Office ohne ausreichende Vorbereitungszeit statt. So ergab eine Wirtschaftsumfrage des Bundesamt für Sicherheit in der Informationstechnik (BSI), dass nur 42 Prozent der Unternehmen auf betriebseigene IT setzen, um die Home-Offices auszustatten. Die Mehrheit folgt dem Konzept, private Geräte betrieblich zu nutzen (BYOD).

IT-Sicherheit ist ein kontinuierlicher Prozess

Nach der Pandemie wird es aber nicht wie früher sein: Viele Beschäftigte werden nicht vollständig ins Büro zurückkehren. Jedes vierte Unternehmen (23 Prozent) will die getroffenen Maßnahmen beibehalten, und weitere vier Prozent möchten sie sogar ausweiten, so der Bitkom.

Draus folgert Arne Schönbohm, Präsident des BSI: „Home-Office ist gekommen, um zu bleiben. IT-Sicherheit ist jedoch noch zu wenig in Budgets, Abläufen und Köpfen der Unternehmen angekommen“. Und Schönbohm betont: „Wer jetzt die Weichen für eine solide Informationssicherheit seiner Infrastruktur legt, der sichert seine Zukunft – in schweren Pandemiezeiten und darüber hinaus.“

Ähnlich beurteilt Achim Berg, Präsident des Bitkom e.V., die Lage: „In der Pandemie sind allein in Deutschland zwölf Millionen Berufstätige ins Home-Office gewechselt. Das ist keine Momentaufnahme, sondern bestimmt dauerhaft die neue Normalität.“ Dabei würde jedoch IT-Sicherheit zu oft keine Rolle spielen: „Für mobiles Arbeiten bedarf es einer Balance zwischen dem benutzerfreundlichen Zugriff auf Unternehmensdaten und dem Schutz der IT. Gefordert sind ein robustes und risikobasiertes IT-Sicherheitsmanagement, Mitarbeiterschulungen und durchdachte Notfallkonzepte. Sicherheit ist kein einmaliges Projekt, Sicherheit ist ein kontinuierlicher Prozess“, so Berg weiter.

Ein neuer „alter Bekannter“: Schatten-IT wächst wieder

Der HP Wolf Security-Report „Out of Sight & Out of Mind” belegt: 36 Prozent der Büroangestellten in Deutschland haben im vergangenen Jahr Drucker und PCs für ihr Home-Office gekauft. Dabei wurde IT-Security oft vernachlässigt, das bestätigten 67 Prozent der deutschen Befragten. So ließen 52 Prozent ihren neuen Laptop oder PC nicht von der Unternehmens-IT prüfen oder installieren, bei Druckern war dies bei 60 Prozent der Fall.

Darüber hinaus nimmt auch die allgemeine Bedrohungslage zu. 57 Prozent der IT-Teams in Deutschland gaben an, dass in den ersten zwölf Monaten der Pandemie Mitarbeiter, die zuhause gearbeitet haben, vermehrt Opfer von Phishing-Attacken wurden. 38 Prozent der Büroangestellten zwischen 18 und 24 Jahren öffneten eine schädliche E-Mail. Dabei gaben 33 Prozent an, dies öfter zu tun, seitdem sie im Home-Office arbeiten.

IT-Security-Support wird schwieriger – und teurer

All das macht den Support komplexer denn je. Laut HP Wolf Security Report verzeichneten 69 Prozent der IT-Abteilungen in Deutschland steigende Wiederherstellungsraten während der Pandemie. Diese korrelieren direkt mit der Anzahl der Endgeräte, die aufgrund einer Kompromittierung gelöscht und neu installiert werden müssen. Die tatsächliche Zahl könnte noch höher liegen: Zwei Drittel der IT-Teams geht davon aus, dass viele kompromittierte Endgeräte noch nicht entdeckt wurden.

So berichteten 69 Prozent der IT-Abteilungen in Deutschland, dass sie mittlerweile viel Zeit investierten, Bedrohungen zu identifizieren. 63 Prozent empfinden es als zeitaufwändiger und schwieriger als vorher, Endgeräte zu patchen und 70 Prozent der deutschen IT-Abteilungen befürchten gar Burnouts und Kündigungen innerhalb ihres Teams.

Der höhere Aufwand schlägt sich auch kostenseitig nieder: Die befragten IT-Teams schätzen, dass die Kosten für den IT-Support seit Beginn der Pandemie um 45 Prozent gestiegen sind.

Damit nicht genug: Vielen Unternehmen ist nicht bewusst genug, welche Ziele Internetkriminelle mittlerweile angreifen. In der von HP durchgeführten Studie „Blurred Lines & Blindspots“ gaben 45 Prozent der IT-Entscheider an, sie hätten in 2020 erlebt, dass ihr Unternehmen über kompromittierte Drucker angegriffen wurden. Die Studie basiert auf Daten von KuppingerCole und 86 Prozent der Führungskräfte gaben an, dass ihre Kunden Bedenken bezüglich der Sicherheit ihrer Heimdrucker haben.

Der Weg zur neuen Endpoint-Sicherheit

Der neue Security-Ansatz muss IT-Sicherheit an jedem Standort gewährleisten können und dazu die Security in die Endgeräte selbst und in die Köpfe der Beschäftigten bringen. Steigende Cyberrisiken müssen standortübergreifend erkannt und abgewehrt werden. Gleichzeitig muss eine Antwort auf den Fachkräftemangel in Support und Security gefunden werden.

Möglich wird dies durch professionelle IT-Lösungen mit integrierter Security, intelligente Security-Services und die Sensibilisierung der Anwenderinnen und Anwender. Diese Security-Maßnahmen können dafür sorgen, dass überall gleich sicher gearbeitet werden kann.

Interview mit Ralf Kleinfeld, Information Security Officer, OTTO

Die „Human Firewall“: der Mensch als Security-Faktor

Anwender werden häufig als „schwächstes Glied in der Cybersecurity-Kette“ bezeichnet. Das sei ein falsches Signal an Beschäftigte, sagt Ralf Kleinfeld, Information Security Officer bei OTTO: Gerade bei der Arbeit im Home-Office kommt es auf den Menschen an. Nur so entstehen Kompetenz und Selbstbewusstsein, um Fälle richtig einzuordnen..

Frage: Zero Trust ist in aller Munde. Sie sagen aber, man sollte in Richtung Maximum Trust gehen. Was meinen Sie damit?

RALF KLEINFELD: Zuerst sollte klar sein: Zero Trust ist kein technisches Produkt, sondern ein Schutz-Konzept. Natürlich erfordert die Umsetzung auf der einen Seite technische Schritte. Auf der anderen Seite spielt der Mensch eine zentrale Rolle, man sollte in der Security immer vom Anwender her denken. Aber nicht, indem man ihm misstraut, sondern indem man ihn stärkt. Wir brauchen mündige Nutzer*innen und keine digitale Sorglosigkeit. Auch bei Zero Trust gibt es Restrisiken und braucht es Restsicherheit, und die muss der Mensch leisten. Hier gilt statt Zero Trust dann Maximum Trust.

*Als Information Security Officer verantwortet Ralf Kleinfeld seit Juli 2013 gesamtheitlich die Aufgabe der Informationssicherheit bei OTTO. Dort ist der MBA, Diplom-Informatiker und Netzwerkexperte seit 2011 in verschiedenen Funktionen tätig. Insgesamt bringt Kleinfeld über 20 Jahre Erfahrung im Security-Bereich mit. Er versteht Informationssicherheit als Haltung, die sich nicht über Produkte kaufen lässt, sondern bei jeder Lösung angemessen und von Beginn an mitgedacht werden muss, ganz im Sinne eines Security-by-Design-Ansatzes. Diesen Anspruch lebt Kleinfeld über die aktive Beteiligung an strategischen Projekten, die sich beispielsweise mit der Weiterentwicklung der Unternehmenskultur oder der Differenzierung von OTTO im Markt beschäftigen. Zudem treibt er das Security-Team-Building in der Organisation voran und fördert das Bewusstsein der Kolleg*innen für Sicherheitsthemen in ihrem Arbeitsalltag mit innovativen Maßnahmen und Formaten.*

Ralf Kleinfeld, Information Security Officer, OTTO

Woher wissen die Anwender, wie sie sich verhalten sollen?

KLEINFELD: Wir geben ihnen Richtlinien an die Hand, die sie in ihren Teams mitgestalten. Sie können aufzeigen, welche Regeln aus ihrer Sicht sinnvoll wären und sagen uns, wo sie sicherheitstechnische Hinweise brauchen.

Das gelingt sogar auf spielerische Art durch sogenannte Skill-Regeln: Wir haben die Sicherheitskompetenzen dokumentiert, die ein Team braucht, und bieten mit einem Tool eine strukturierte Herangehensweise an, um dort hinzukommen. Auf diese Weise ist dafür gesorgt, dass die Sicherheitsansätze zur Kritikalität unserer Prozesse und Daten passen. Dieser Prozess macht die Teams eigenständig und wir sichern am Ende die Qualität.

Sie wollen also Nutzer einbeziehen und nicht nur Security verordnen. Richtig?

KLEINFELD: Genau. Der bessere Weg ist, Informationssicherheit in der Unternehmenskultur zu verankern. Das funktioniert bei OTTO deshalb sehr gut, weil Digitalisierung Teil unserer Kultur ist. Wir haben schon länger Grundsätze formuliert wie Eigenverantwortung und kontinuierliche Weiterentwicklung, die nun auch für die Informationssicherheit gelten.

Dass wir Informationssicherheit aus der isolierten Expert*innen-Sicht herausheben, halte ich für entscheidend. Informationssicherheit ist ein fester Bestandteil von Digitalisierung – auch wenn wir natürlich wissen, dass nicht alle Expert*innen darin sind.

*„Es ist entscheidend, dass wir Informationssicherheit aus der isolierten Expert*innen-Sicht herausheben."*

Ralf Kleinfeld, ISO bei OTTO

Was heißt das konkret in der Umsetzung?

KLEINFELD: Mit meinem Team versuchen wir, andere zu sensibilisieren und zu schulen. Die Kolleg*innen sollen lernen, selbst festzustellen, ob sie es mit einem Sicherheitsvorfall zu tun haben. Wenn sie sich unwohl fühlen, unsicher sind und glauben, da sei etwas Eigenartiges passiert, dann tun wir das nicht ab, sondern betrachten es immer als Sicherheitsvorfall.

Ich will davon weg, dass die Kolleg*innen sagen: ‚Das ist bestimmt etwas ganz Banales oder vielleicht sogar mein eigener Fehler. Ich weiß nicht, ob ich das melden sollte.' Sie sollen sich freimachen davon zu glauben, sie könnten uns unnötigerweise beschäftigen.

Wenn sie sagen: ‚Hier stimmt etwas nicht', dann ist das für uns erst einmal ein Sicherheitsvorfall. Wir überlegen dann zusammen, ob das tatsächlich so ist, und prüfen, wie wir sie unterstützen können, sich sicherer zu fühlen.

Wie wirkt sich das aus?

KLEINFELD: Es entsteht mehr und mehr Kompetenz und Selbstbewusstsein, um Fälle richtig einzuordnen. Die Beschäftigten lernen ständig dazu und fühlen sich kompetenter. Beim nächsten Mal müssen sie sich dann vielleicht gar nicht mehr melden.

So etwas kommt nicht über Nacht, aber insgesamt stellen wir uns damit resilienter auf. Nehmen wir das Beispiel Luftfahrt: Dort weiß man heute, dass Flugzeugabstürze selten die Konsequenz von einem Ereignis sind, sondern aus einer Kette von Ereignissen.

Das lässt sich auf Informationssicherheit übertragen: Ziel muss es sein, die Kette frühzeitig zu unterbrechen. Jedes einzelne Event ist eine Chance, um den Vorfall oder GAU zu verhindern. Dafür brauchen wir aber viele Sensoren. Die haben wir technologisch mit Monitoring und einem Informationssicherheitsteam, aber die Organisation selbst

braucht auch Sensoren. Und Menschen werden desto wertvoller als Sensoren, je besser sie ausgebildet und sensibilisiert sind. So können sie helfen, die Kette zu unterbrechen.

> *„Um einen Vorfall zu verhindern, braucht auch die Organisation selbst Sensoren."*
>
> **Ralf Kleinfeld, ISO bei OTTO**

Wie ordnen Sie die Technik als Sicherheitsfaktor ein und wie den Menschen?

KLEINFELD: Was Technologie heute an Schutz bieten kann, ist bekannt und gut ausgereift. Vollständig wird dieser Schutz nie sein. Die Lücken in den Technologien zu finden, ist das Geschäft von Kriminellen.

Und um dem zu begegnen, brauchen Mitarbeitende technische und sicherheitsspezifische Kompetenz. Banales Beispiel: Landet eine Phishing-Mail im Postfach, hat die Technologie sie nicht erkannt und versagt. Also müssen die Mitarbeitenden die Mail richtig beurteilen und reagieren.

Gerade mit Blick auf Hybrid Work und die vermehrte Tätigkeit in Mobile-Offices, müssen wir die Anwender befähigen, damit sie sich auch in Situationen, in denen sie alleine sind, sicher fühlen.

Wenn letztlich alle Beschäftigten Aufgaben in der Security übernehmen, sollte dies entsprechend bewertet werden?

KLEINFELD: Absolut! Security hat einen Wert für das Unternehmen. Die Leistungen, welche die Beschäftigten erbringen, sind nicht einfach ein Erfolg für die Security, sie sind ein Erfolg für das Unternehmen.

Es gibt Missverständnisse zu Security, die Unternehmen bei sich beseitigen sollten: So ist Security kein reines Expert*innen-Thema, sondern ein Thema der Unternehmenskultur, ein Thema für die Unternehmensleitung und alle Beschäftigten. Es ist auch kein Projekt und hat kein definiertes Ende, Security ist fortlaufend ein Thema, eine Daueraufgabe.

Last but not least: Nicht die IT sollte den Schutzbedarf bestimmen, sondern die Fachabteilungen. So sind bereits Unternehmen dadurch in ihrer Produktivität stark beeinträchtigt worden, weil die Fax-Geräte nicht mehr funktionierten. Aus einer technologischen Bewertung ist ein Fax-Gerät möglicherweise nicht sehr relevant, für die Fachabteilungen, in Geschäftsprozessen und damit den Unternehmenserfolg womöglich aber sehr!

Interview mit Alexander Dorn, Director End User Sales Personal Systems, HP

Dorn verantwortet bei HP Deutschland den Endkundenvertrieb der Sparte Personal Systems. Er ist seit 2000 bei HP tätig und hat verschiedene Finanz- und Vertriebspositionen ausgeübt und blickt auf mehr als 10 Jahre Führungserfahrung zurück.

„Rechne immer mit etwas Unerwartetem und sei darauf vorbereitet“

Hybrid Work gilt als die neue Form des Arbeitens. Deshalb sollte die Zeit des Experimentierens vorbei sein, erläutert HP-Experte Alexander Dorn. Jetzt sind grundlegend neue Konzepte gefragt – und eine fundierte Vorbereitung auf den Ernstfall.

Als es so schnell ins Home-Office ging, mussten zahlreiche Mitarbeiter private Geräte nutzen. Und viele bleiben noch im Einsatz. Wie kann man dabei für sichere Endgeräte sorgen?

DORN: Mit so einer Situation hatte niemand gerechnet. Aber dass stets etwas Unerwartetes passieren kann, ist ja typisch für IT-Sicherheit. Heute haben wir einiges daraus gelernt. Zum Beispiel mit neuen Angriffsflächen umzugehen. Das Internet ist Teil des Unternehmensnetzwerks geworden und damit sind Schwachstellen erreichbar, die früher nicht zugänglich waren. Zudem entsteht eine neue, vielfältige Schatten-IT. Oft wird zum Beispiel eine private Webcam für Online-Meetings genutzt oder der Heimrouter für den Internetzugang. Von diesen Geräten hat die IT keine Kenntnis, sie kann nicht ihre Sicherheit bewerten. Das gilt selbst, wenn ein Firmen-Notebook im Home-Office bereitsteht. Damit hat die IT heute eine neue Aufgabe, die vergrößerte Angriffsfläche zu minimieren.

Eine Herausforderung für viele IT-Abteilungen

DORN: Natürlich war und ist das eine kritische Situation. Zumal es noch einen „Bruch“ gibt zwischen Nutzern und IT-Abteilung. Sie arbeitet heute räumlich getrennt von den Anwendern, die gerade jetzt viel Support benötigen. Die IT ist nicht mehr so einfach zu erreichen wie in klassischen Bürozeiten.

Unter dem Strich bedeutet das alles: Endpoints müssen Angriffen widerstehen können – möglichst ohne die Unterstützung der IT-Abteilung.

Das ist eine neue Sichtweise auf Endpoint-Security. Wie kann die IT hier vorgehen?

DORN: Oft richten sich die Blicke darauf, wie man Angriffe erkennen kann. Man überlegt, wie man Vorfälle möglichst schnell detektiert und sich vor ihnen schützt.

Das ist nur die halbe Miete. Wir müssen ja davon ausgehen, dass es zu Vorfällen kommen wird. Daher gehört es in aller Regel dazu, die betroffenen Endpoints wiederherzustellen. Das ist wichtig. Jede Stunde, die ein Endpoint ungenutzt bleibt, senkt die Produktivität, ein großer Schaden für das betroffene Unternehmen. Die Wiederherstellbarkeit der Endpoints wird häufig noch vergessen

Wie soll das geschehen? Schickt man die IT-Abteilung in die Home-Offices, um Notebooks wiederherzustellen? Oder soll man Ersatz-Notebooks

DORN: Es ist offensichtlich: Das dauert zu lange und ist mit einem zu hohen Aufwand verbunden. Auch hier ist die Lösung: Endpoints müssen selbst dafür sorgen können, dass die Wiederherstellung schnell gelingt.

HP Endpoints zum Beispiel bieten die Funktion Sure Recover. Mit dieser Hardware-gestützten Wiederherstellung können Anwender schnell und einfach ein neues Image auf ihrem Gerät installieren und so selbst dafür sorgen, dass sie nach einem Vorfall weiterarbeiten können.

> *„Nach einem Vorfall müssen Endpoints schnell wiederherstellbar sein“*
>
> **Alexander Dorn, HP**

Das klingt ein wenig nach Zero-Trust-Konzept. Hilft das bei Hybrid Workplaces?

DORN: Ja, über Zero Trust wird viel gesprochen, auch in Verbindung mit Hybrid Work. Es geht immer darum, dass Unbefugte keine Berechtigungen erhalten, um Daten auszuspähen und zu missbrauchen. Man kann Zero Trust aber falsch verstehen. Wenn man möglichst niemanden Berechtigungen erteilt, um unbefugte Dritte fernzuhalten, erschwert das die Arbeit der Beschäftigten. Sie werden stark limitiert, was sie machen dürfen.

Nun sind wir Menschen aber kreativ. Nutzer suchen nach Auswegen, wie sie zum Beispiel trotz blockierter USB-Schnittstellen doch einen externen Speicher an ihr Notebook anschließen können. So etwas war im Büro nicht so leicht, aber im Home-Office können sich Nutzer mehr Auswege überlegen.

Deshalb erfordert Zero Trust nicht nur die risikoabhängige Vergabe von Berechtigungen, sondern auch, das Bewusstsein der Beschäftigten durch Awareness-Trainings zu schärfen.

Zero Trust hat aber einen Schwachpunkt: Wer es zu starr umsetzt, bekommt zu viele Warnungen.

DORN: Das stimmt. Wird Zero Trust zu rigide umgesetzt, werden viele an sich legitime IT-Prozesse zu Warnungen führen, die untersucht, bewertet und bearbeitet werden müssen. Dafür fehlt aber Personal, der Fachkräftemangel in der Security verschärft sich immer weiter. Auch KI kann dies nicht verhindern, denn auch sie treibt die Zahl der Sicherheitswarnungen in die Höhe, darunter auch viele False Positives.

Besser ist es deshalb, die Endpoints selbst mit Sicherheit auszustatten, die ohne die IT-Abteilung auskommt. Deshalb empfehlen wir als weitere Sicherheitsebene die Isolation der einzelnen Anwendungen auf den Endpoints. Eine solche Mikro-Virtualisierung bietet zum Beispiel HP Sure Click. Wird eine Datei geöffnet, geschieht dies in einem geschützten Bereich. Befindet sich eine Malware in der Datei, kann diese nicht ausbrechen und keinen Schaden anrichten. Die Isolation mit HP Sure Click arbeitet überall, ist ideal für Hybrid Work und entlastet die Security-Fachkräfte, denn der Schutz wirkt automatisch.

Wir haben jetzt über neue Konzepte und neue Tools gesprochen. Wie wird sich Security künftig entwickeln?

DORN: Cybergefahren sind im Jahr 2022 die größte Sorge für Unternehmen weltweit, so das neue Allianz Risk Barometer 2022. Die Bedrohung durch Ransomware-Angriffe, Datenschutzverletzungen oder IT-Ausfälle beunruhigt die Unternehmen sogar noch mehr als Geschäfts- und Lieferkettenunterbrechungen, Naturkatastrophen oder die Covid-19-Pandemie, die alle Unternehmen im vergangenen Jahr stark beeinträchtigt haben.

Daher werden die Budgets dafür weiter wachsen, aber es müssen die richtigen Konzepte umgesetzt werden, damit diese Ausgaben wirken. Security als Antwort auf die Cybergefahren darf deshalb nicht mehr nur als Aufgabe der IT gesehen werden. Wenn es um die Bewältigung des größten Unternehmensrisikos geht, ist das ganze Unternehmen und die Unternehmensleitung gefragt. Security ist deshalb keine IT-Aufgabe, sondern eine Unternehmensaufgabe. Das muss in Zukunft ganz klar werden.

DLG verbessert die Mitarbeiter-produktivität und reduziert die IT-Administration

Als offenes Netzwerk und fachliche Stimme der Land-, Agrar- und Lebensmittelwirtschaft will die DLG, die mehr als 30.000 Mitglieder hat, das Fachwissen fördern, für einen breiten Transfer von Technologie und Know-

how sorgen, aber auch Qualitätsmaßstäbe setzen und sichern. Die DLG testet Lebensmittel sowie Landtechnik und Betriebsmittel in eigenen Testzentren. Außerdem veranstaltet sie weltweite Leitmessen wie die AGRITECHNICA und die EuroTier sowie mehr als 40 Ausstellungen in zahlreichen Ländern.

Diese Aufgaben stemmen DLG-Mitarbeiter und Ehrenamtliche in mehr als zehn Ländern. Dafür werden sie von der neunköpfigen IT mit Endgeräten ausgestattet. In der Vergangenheit handelte sich hier um eine sehr heterogene Geräteflotte, bestehend aus Desktop-PCs, kleineren und größeren Notebooks, All-in-one-Geräte, Tablets – und zwar unterschiedlichen Alters. „Für uns in der IT war das Management der Clients mit einem großen Aufwand verbunden“, erinnert sich Holger-Steffen Stapf, IT-Leiter der DLG. „Wir mussten uns damit befassen, welcher Mitarbeiter welches Endgerät erhält, wie alt die einzelnen Endgeräte sind und wann sie ausgetauscht werden müssen.“

Die Anforderungen der Mitarbeiter an die Hardware war außerdem sehr unterschiedlich: Manche wollten tragbare Geräte, andere Desktop-PCs, manche wollten mit Stift, andere ohne arbeiten. „Hinzu kamen für uns natürlich das Monitoring der Geräte, das Patchen und die entsprechenden Security-Maßnahmen. Daher stand für uns fest, dass wir die Arbeit in der IT durch eine rigorose Standardisierung reduzieren mussten“, so Stapf. Das Ziel lautete: Nur noch ein Typ von Endgerät, das allen Anforderungen entspricht, das optisch gut ausschaut und einen ordentlichen Support im Hinblick auf Produktivität und Sicherheit hat.

LÖSUNG: HP Device as a Service mit Proactive Insights und HP Wolf Pro Security Service

Stapf konsultierte das IT-Systemhaus MCL IT GmbH, mit dem die DLG in der Vergangenheit bereits zusammengearbeitet hat. MCL IT GmbH macht zwei Angebote – einmal mit Hardware des bisherigen Hardware-Lieferanten und einmal mit HP-Geräten. „Für uns war schnell klar, dass wir den Wechsel zu HP wollten, da HP mit HP Device as a Service mit seinen proaktiven Endpunkt-Management-Services und -Analysen deutlich mehr bot als reine Hardware“, sagt Stapf.

Das heißt, die DLG bezieht die Hardware und die Tools für das Management im As-a-Service-Modell von HP, um den Rest kümmert sie sich selbst. Die Wahl fiel im ersten Schritt auf HP EliteBook x360 Notebooks mit Docking-Station und Displays, ergänzt durch HP Financing und HP Proactive Insights. HP Proactive Insights inventarisieren und überwachen die Endgeräte und liefern der DLG in einem HP TechPulse-Dashboard vorausschauenden Analysen. So werden Probleme proaktiv erkannt und behoben, bevor sie überhaupt auftreten. Stapf: „HP Proactive Insights liefert Antworten auf Fragen wie: Sind die Geräte richtig ausgelastet? Ist die richtige Auswahl an Geräten getroffen worden oder benötigt der ein Mitarbeiter ein leistungsstärkeres Gerät?“ Später hat die DLG das Paket um HP Wolf Pro Security Service1 ergänzt. „Damals machten Hacker-Angriffe die Runde und unsere Geschäftsführung wollte von mir über den Security-Status unserer IT-Infrastruktur informiert werden. Ich habe damals berichtet, dass HP über eine neue faszinierende Technologie verfügt, die unsere Client-Infrastruktur wesentlich sicherer macht. Das kam bei der Geschäftsführung sehr gut an“, erinnert sich Stapf.

Durch eine Kombination von zwei intelligenten und sich ergänzenden Technologien – Deep Learning und Microvirtualisierung – bietet HP Wolf Pro Security Service proaktiven, mehrstufigen Echtzeitschutz für die Endgeräte.

„Wir wollten den Wechsel zu HP, da HP mit HP Device as a Service mit seinen proaktiven Endpunkt-Management-Services und-Analysen deutlich mehr bietet als reine Hardware.“

Holger-Steffen Stapf, IT-Leiter, DLG

Geschäftsergebnisse: Den Zustand und die Sicherheit der Geräte immer im Blick

„Unserer Finanzabteilung gefällt das HP Device as a Service Modell sehr gut, da wir für die Clients nun einen monatlichen Fixpreis für Hardware plus Service-Leistungen zahlen“, sagt Stapf. Doch auch für die Mitarbeiter und die IT-Abteilung der DLG hat der Umstieg auf HP und das Service-Modell Vorteile: „Sämtliche Clients sind immer technologisch aktuell. Dabei müssen wir uns auch nicht mehr darum kümmern, was mit den Geräten am Ende des Lifecycles geschieht“, so Stapf.

„Von großem Vorteil sind für uns HP Proactive Insights, denn damit kennen wir jetzt den Zustand aller Geräte genau“, erklärt Stapf. „Früher haben wir zum Beispiel direkt von den Endanwendern erfahren, wenn der Akku eines Notebooks schwächer wurde. Jetzt können wir proaktiv handeln – und im Fall eines Geräteaustauschs schickt HP einen Service-Techniker zu dem jeweiligen Mitarbeiter, ganz gleich, wo er auf der Welt ist. Wir müssen dafür nur ein Ticket bei HP eröffnen. So einfach geht das.“ Die HP TechPulse Analysen liefern der DLG zudem Informationen zu neuen Treibern oder Patches etwa von HP oder Microsoft. „Das war früher ein manueller Prozess.

Heute erledigt HP diese Arbeit für uns, dadurch sparen wir rund 10 % Administrationsarbeit“, freut sich Stapf. Durch Proactive Insights hat die DLG die Zahl der Geräteausfälle um mehr als 15 % gesenkt, sodass die Mitarbeiter in der IT deutlich entlastet sind. Auch wurde dadurch die Produktivität der Mitarbeiter gesteigert.

HP Wolf Pro Security Service in Kombination mit den HP Elitebook x360 Notebooks haben es zudem ermöglicht, dass alle Mitarbeiter zu Beginn der Corona-Pandemie schnell ins Homeoffice wechseln konnten. Stapf: „Die Geräte sind besser vor Hackerangriffen geschützt, obwohl sie nicht mehr dahinterstehen unsere Firewall.“ Dies eröffnet der DLG künftig auch die Chance, bei großen Messen auf teure Standleitungen zu verzichten und die Geräte stattdessen über eine Internet-Verbindung ans Netzwerk anzubinden. „Die Geräte wären dank der HP-Tools und -Services sicher“, so Stapf.

DIE LÖSUNG AUF EINEN BLICK:

HP Services and Solutions:
HP Device as a Service
HP Proactive Insights powered by HP TechPulse HP Wolf Pro Security Service
HP Financial Services

Hardware:
HP EliteBook x360 Notebooks
mit Docking-Station und Displays

Weitere Informationen

Erfahren Sie, wie sich Cyberattacken direkt auf dem Endpoint und an jedem Standort mit einem Isolierungskonzept erkennen und eindämmen lassen. Lesen Sie jetzt das Whitepaper „EIN NEUES MODELL, DAS VOR CYBERANGRIFFEN SCHÜTZT UND GLEICHZEITIG KOSTEN SENKT“

Zum Whitepaper

Hybrid Work erfordert Zero Trust, um an jedem Standort für Endpoint Security sorgen zu können. Wie Sie mit HP Wolf Security das Zero-Trust-Konzept erfolgreich umsetzen und Hybrid Work so besser schützen, lesen Sie in dem Whitepaper „ZERO-TRUST MIT HP WOLF ENTERPRISE SECURITY“

Zum Whitepaper