

G DATA Report



Homeoffice in der Corona-Pandemie:



Dauerhaft sicher!

Vorwort

„Meistens kommt es anders als man denkt.“

Dieser Satz gilt im besonderen Maße für das Jahr 2020. Ein Jahr, das spätestens seit Mitte März im Krisenmodus ist. Und Geschäfts- und Privatleben grundlegend auf den Kopf gestellt hat. Und eines ist sicher: Die Coronakrise wird unser Leben auf vielen Ebenen nachhaltig verändern. Die erzwungene Digitalisierung hat in vielen deutschen Unternehmen dazu geführt, dass von heute auf morgen nahezu alle Mitarbeiter sich im Homeoffice wiederfanden.

Aus Sicht der IT-Sicherheit ein gewagtes Unterfangen. Denn bei allen Bestrebungen, Angestellten einen direkten Zugang ins Unternehmen zu ermöglichen, haben viele IT-Verantwortliche einem Aspekt nicht genügend Aufmerksamkeit gewidmet:

Denn die Erfahrung der letzten Monate zeigt: Vorbeugen ist immer besser und günstiger, als im Incident adäquat zu reagieren.

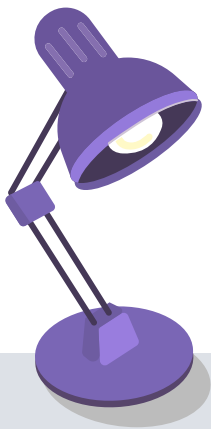
Der **IT-Sicherheit**. Denn „schnell, schnell“ ist für ein sicheres Netzwerk keine adäquate Vorgehensweise.

In diesem Paper zeigen wir

- wie Cyberkriminelle die aktuelle Pandemie für sich ausnutzen
- wie Corona, Homeoffice und IT-Sicherheit zusammenhängen

Wir geben Ihnen Tipps

- wie ihre Mitarbeiter sicher von zu Hause aus arbeiten können
- wie Unternehmen ihre IT-Sicherheit zukunftsfähig aufstellen sollten



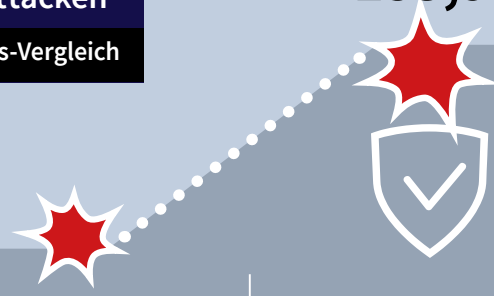
Abgewehrte
Cyber-Attacken

im Quartals-Vergleich

+ 153,9 %

Quartal 1

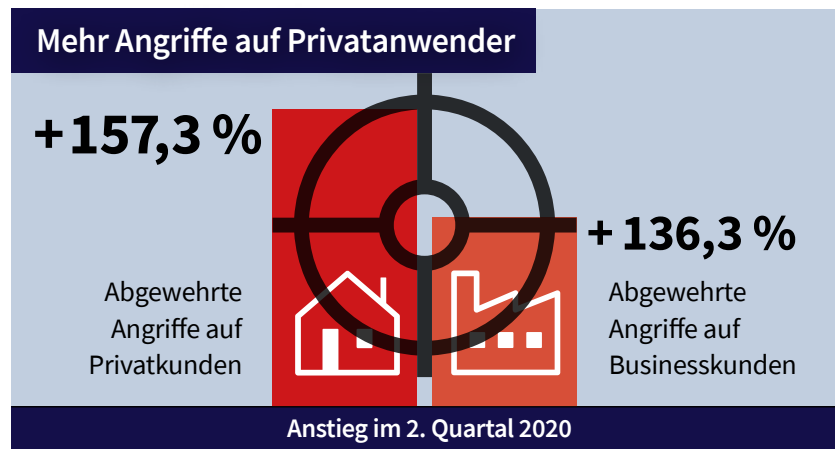
Quartal 2



Die aktuelle Bedrohungslage

Massive Zunahme: Zahl der Cyberattacken steigt deutlich

Die aktuelle Bedrohungsanalyse von G DATA CyberDefense belegt: Cyberkriminelle nutzen die Coronakrise aus und attackieren Privatanwender und Unternehmen. Bereits im März hat die Zahl der abgewehrten Angriffe um **30 Prozent** zugenommen. Zu Beginn der Coronakrise haben kriminelle Hacker vermehrt E-Mails verschickt, die etwa neue Corona-Tracker oder günstige Atemschutzmasken versprochen haben.



Im zweiten Quartal standen Privatanwender **verstärkt im Visier von Cyberkriminellen**. Auch wenn mittlerweile viele Angestellte aus dem Homeoffice an ihren Büro-Arbeitsplatz zurückgekehrt sind, verbringen die Menschen privat viel mehr Zeit am Computer. Um etwa Online zu shoppen oder einen Lieferdienst für Essen zu beauftragen. Die Angriffsfläche ist durch die **gestiegene**

Onlinenutzung deutlich größer geworden. Die Zahl der abgewehrten Angriffe stieg im zweiten Quartal im Vergleich zum ersten um **mehr als 157 Prozent**. Aber auch Unternehmen stehen weiterhin unter Beschuss. **136,3 Prozent** mehr Angriffsversuche auf Firmennetzwerke verzeichneten die Cyber-Security-Experten von G DATA zwischen April und Juni.

Die aktuelle Bedrohungslage

Im ersten Halbjahr haben Cyberkriminelle das Tempo weiter erhöht und versucht, ihren Schadcode in **immer kürzeren Abständen** mit Packern vor Antiviren-Lösungen zu verstecken. So haben die Experten von G DATA bei einigen Malware-Familien bereits im ersten Halbjahr mehr neu verpackte Varianten entdeckt als im vergangenen Jahr insgesamt.

Bei Trickbot hat sich die Zahl sogar fast **verdreifacht**. Durchschnittlich alle 6,5 Minuten haben die Kriminellen ein neues Trickbot-Sample veröffentlicht und versucht, Computer und Netzwerke zu infiltrieren. Der Remote Access Trojaner njRAT/Bladabindi hat bereits nach sechs Monaten so viele neue Samples wie im gesamten vergangenen Jahr.

Die Malware-Top 10 (Januar bis Juni 2020)

im Überblick:



Platz	Name	Varianten	Art
1	Trickbot	40.265	Malware Distributor
2	njRAT/Bladabindi	39.521	Remote Access Trojaner
3	QBot/Qakbot	29.677	Remote Access Trojaner
4	Emotet	27.804	Malware Distributor
5	RemcosRAT	24.845	Remote Access Trojaner
6	SakulaRAT	23.158	Remote Access Trojaner
7	BlackShades	21.241	Remote Access Trojaner
8	Tinba	20.881	Banking-Trojaner
9	AgentTesla	19.060	Information-Stealer
10	AMRat	17.149	Remote Access Trojaner

Cyberkriminelle nutzen vielfältige Methoden, um Unternehmensnetzwerke und Privatrechner zu infiltrieren und für ihre Zwecke zu missbrauchen. Dabei gehen sie häufig den Weg des geringsten Widerstands und nutzen Lücken in Betriebssystemen oder Anwendungen aus. [Auch der Mensch ist weiterhin ein Einfallstor für Angriffe, wenn er in Phishing-Mails Links anklickt oder Anhänge öffnet, die Schadcode enthalten.](#)

Welche Gefahren drohen im Homeoffice?

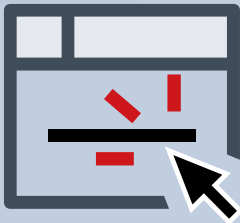
Gefährliche E-Mail-Anhänge



Wer würde schon eine vermeintliche Mail vom Chef oder IT-Kollegen ignorieren, die einen Anhang mit dem Namen „**COVID-19-Neue_Home_Office_Regelung_Ab_Juni.doc**“ enthält? Oder die scheinbar wichtige Regelungen von der WHO oder einer Gesundheitsbehörde verkündet? Kriminelle verschicken aktuell vermehrt täuschend echte E-Mails mit gefährlichen Anhängen. Sobald jemand den Anhang öffnet, wird eine **Spionagesoftware** auf dem PC installiert.

Oder das Gerät wird durch **Ransomware** komplett verschlüsselt. Damit es wieder entschlüsselt wird, fordern die Kriminellen hohe Geldsummen von ihren Opfern.

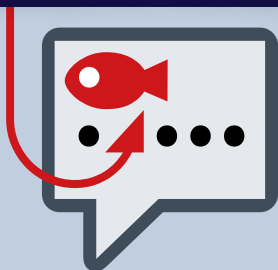
Bösartige Links



Über Social Media und E-Mails verbreiten Kriminelle **Fake-News** über angeblich fertige Impfstoffe, Sonderangebote zu Schutzmasken oder irreführende Ratschläge.

Nutzer sollen auf einen Link klicken. Dieser führt jedoch zu einer **bösartigen Webseite**, die unbemerkt Schadsoftware auf den PC lädt.

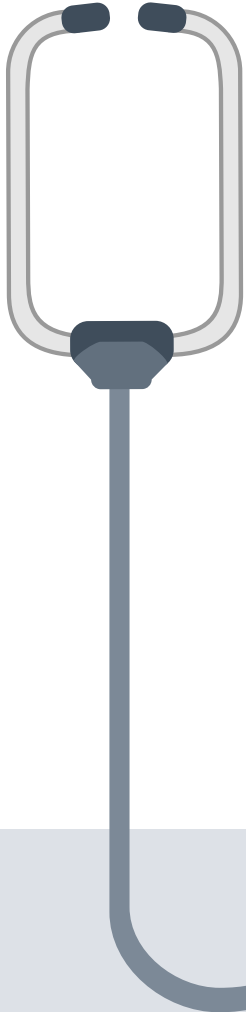
Datenklau mit Phishing



In betrügerischen Nachrichten per E-Mail oder in Social Media fordern Kriminelle die Nutzer auf, **vertrauliche Daten** offenzulegen, etwa Passwörter, Zugangsdaten oder Kreditkartennummern. Dazu sollen sie auf einen Link klicken und dort die Daten eingeben. Diese Links führen jedoch auf **gefälschte** und zumeist **täuschend echt aussehende Webseiten**, auf denen die Daten abgegriffen werden.

Schnell können sich Kriminelle so Zugang zum Unternehmen erschleichen, etwa zu vertraulichen Dokumenten des Arbeitgebers.

Was Corona mit IT-Sicherheit zu tun hat



Das Covid-19-Virus verunsichert immer noch weltweit ganze Gesellschaften und legt Teile der Wirtschaft lahm. Dabei gibt es zwischen dem Virus und üblichen Problemen der Cybersecurity zahlreiche Gemeinsamkeiten. Und auch die empfohlenen Abwehrmaßnahmen sind nicht soweit von Expertentipps im Bereich IT entfernt.

Viele infizierte Personen zeigen lange keine Symptome, sind aber trotzdem Träger des Virus. Und auch wenn viele infizierte Personen nur einen leichten Krankheitsverlauf haben, gibt es trotzdem zahlreiche Todesfälle zu beklagen.

Genauso ist es mit ungezählten **Cyberangriffen** – besonders im Unternehmensumfeld: Im IT-Umfeld werden zahlreiche Infektionen oft lange nicht erkannt, weil

Cyberkriminelle nach einem erfolgreichen Angriff oft erst einmal gar nichts tun – um nicht erkannt zu werden. Die Infektion bleibt somit symptomfrei, während sich die Kriminellen längst im Netzwerk breitgemacht haben.

Hier ergibt sich eine weitere Parallele: Wenn ein Experte nicht entweder zufällig über bestimmte Indikatoren stolpert oder gezielt nach diesem Ausschau hält, wird die Infektion erst bei Ausbruch erkannt – und dann ist es oft zu spät. [So lauert eine Malware wie Emotet – eine der gefährlichsten Malware-Familien – oft wochenlang im Netz und liest Informationen aus dem Netzwerk aus.](#)



Die Infektion wird oft erst dann sichtbar, wenn Kriminelle sich entscheiden, ihren Angriff etwa durch Aufspielen einer Ransomware wie Ryuk, STOP Ransomware oder Sodinokibi zu monetarisieren.

[Nach Expertenschätzungen dauert es im Schnitt noch immer mehrere Monate, bis eine Infektion das erste Mal bemerkt wird.](#)

Was Corona mit IT-Sicherheit zu tun hat

Doch was hat das mit Corona zu tun?



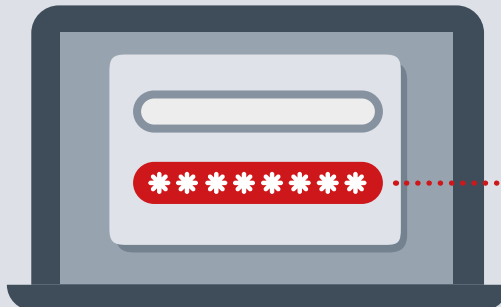
Um eine Infektion mit der Grippe oder auch dem Covid-2019-Virus zu verhindern, empfehlen Gesundheitsexperten vor allem eins: eine vernünftige **Hygiene**. Denn regelmäßiges, gründliches Händewaschen zerstört einen der häufigsten Eintrittsvektoren für Viren – die Schmierinfektion. Ebenfalls hilfreich ist es, sich nicht mit den Händen ins Gesicht zu fassen. Denn sonst kann das bösartige Virus auf die Schleimhäute der Atemwege überspringen und so die eigentliche Infektion auslösen.



Doch wer dazu einen Selbstversuch startet, merkt schnell, dass das gar nicht so einfach ist. Sich jahrelang antrainierte Handlungen abzugewöhnen, geht nur mit starker Willenskraft – und **regelmäßiger Wiederholung**. [Ähnlich sollten Unternehmen vorgehen,](#)

[wenn sie ihre Mitarbeiter zur menschlichen Firewall ausbilden wollen.](#) Damit wird der einzelne Mitarbeiter kein Sicherheitsproblem, sondern zum **stärksten Teil** des Verteidigungskonzeptes. Nur wenn Mitarbeitende immer wieder mit möglichen Phishing-Mails konfrontiert werden und gesperrte Workstations eine Selbstverständlichkeit sind und keine Ausnahme, beginnt sich eine **Sicherheitskultur** im Unternehmen zu etablieren.

Was übrigens auch zur selbstverständlichen Hygiene gehören sollte – ähnlich wie das Wechseln von Einmalhandschuhen im medizinischen Bereich – ist der **Umgang mit Passwörtern**. Dabei kommt es nicht einmal darauf an, diese regelmäßig zu ändern – was der Sicherheit sogar schaden kann.



Vielmehr sollten Nutzer sich bewusst machen, dass mehrfach verwendete und schlecht gewählte Passwörter es Angreifern unnötig einfach machen, ihre Accounts zu übernehmen.

Empfehlenswert ist daher die Verwendung einzigartiger, zufallsgenerierter Passwörter – die dann idealerweise in einem **Passwortmanager** gesichert werden.

Was Corona mit IT-Sicherheit zu tun hat



Und auch das Überspringen des Virus von der Hand auf die Atemwege aus unserem Beispiel ist etwas, das Unternehmen unterbinden können. Denn wer vorsorgt, kann im Unternehmen durch **Segmentierung von Netzwerken** dafür sorgen, dass eine Infektion in der Personalabteilung nicht auf das Produktionsnetzwerk oder den Bereich Research and Development überspringen kann.

So wird ein Sicherheitsvorfall zwar nicht vollständig verhindert, aber seine Auswirkungen wirksam begrenzt.

Aufmerksam statt ängstlich

Genau wie bei Corona gilt übrigens auch in der IT-Sicherheit: **Panik ist immer ein schlechter Berater**. Und leider gibt es viel zu viele vermeintliche Experten, deren Ratschläge – vorsichtig gesagt – nicht zielführend sind.

Natürlich haben sowohl Schutzsoftware als auch Gesichtsmasken ihre Daseinsberechtigung – aber nicht in der Form, in der sie von Unkundigen eingesetzt werden. Das Tragen von einer Gesichtsmaske allein

verhindert eine Infektion mit Covid-19 ebenso wenig wie eine Firewall allein vor dem Öffnen eines infizierten Mailanhangs schützt. Wer sich ausschließlich auf diese Maßnahmen verlässt, ist schlecht beraten und steht einer Infektion ungeschützt gegenüber.





Vielmehr hilft ein durchdachtes Sicherheitskonzept dabei, die **Angriffsfläche** für Viren und andere Schädlinge zu **minimieren**. In der IT-Sicherheit genau wie in der Medizin.

So klappt's mit dem sicheren Homeoffice


Homeoffice ist auch heute ein vernünftiger Schritt, der die Ausbreitung des Virus innerhalb der Bevölkerung verlangsamt. Dank der technischen Ausstattung ist der Umstieg auf Heimarbeit für viele Unternehmen zudem kein unüberwindbares Problem mehr.


Im Folgenden finden Sie einige **Tipps für Ihre IT-Abteilung**, um die Heimarbeit so sicher und reibungslos zu gestalten wie möglich:





-  **Ermitteln Sie, welche Funktionen innerhalb des Unternehmens absolut unverzichtbar sind** und wo ein Ausfall negative Folgen für das Unternehmen hätte. Die MitarbeiterInnen, die auf diesen Positionen arbeiten, sollten als erstes die Möglichkeit bekommen, vom Homeoffice aus zu arbeiten.
-  **Stellen Sie den Mitarbeitern für die Heimarbeit firmeneigene Geräte zur Verfügung.** Firmendaten haben auf Privatgeräten nichts zu suchen. Ebenso sollten Privat-PCs niemals über VPN ins Firmennetz gestellt werden, da niemand gewährleisten kann, dass alle Rechner die Sicherheitsvoraussetzungen erfüllen.
-  **Aktivieren Sie auf Homeoffice-Geräten die Festplatten-Verschlüsselung.** So führt selbst der Verlust eines Gerätes nicht zu einem Datenschutzproblem.
-  **Stellen Sie ein VPN für die Verbindung ins Firmennetz zur Verfügung.** So macht es keinen Unterschied, ob ein/e Mitarbeiter/in im Büro oder am heimischen Schreibtisch sitzt. Hier ist zuerst die IT-Abteilung gefragt, die die Zugänge lizenzieren, einrichten und bereitstellen muss.


So klappt's mit dem sicheren Homeoffice

 **Aktivieren Sie die Mehrfaktoranmeldung für das VPN.** Auch dies ist Aufgabe der IT-Abteilung. Es gibt verschiedene Möglichkeiten, vom Einsatz von Hardware-Tokens zum Beispiel in Form eines USB-Sticks bis zur OTP-App. Diese generieren für jede Anmeldung ein einmaliges und nur für die jeweilige Anmeldung gültiges Passwort.

 **Definieren Sie klare Anforderungen für Zugriffe.** Ein VPN-Zugang nützt nichts, wenn ein Mitarbeiter/eine Mitarbeiterin nicht auf Dateien innerhalb des Netzwerkes zugreifen bzw. Anwendungen remote nicht nutzen kann.

 **Konfigurieren Sie (falls vorhanden) auch die VoIP-Telefonie so, dass sie aus der Ferne funktioniert.** Alternativ: Richten Sie entsprechende Rufumleitungen ein.

 Falls es nicht möglich ist, dem jeweiligen Mitarbeiter ein entsprechend vorkonfiguriertes Notebook zur Verfügung zu stellen: **Auch ein Remote-desktop-Server (auch Terminalserver genannt) ist im Notfall eine gangbare Lösung.** Hier gilt es nur, entsprechende Serverkapazitäten und ausreichend Bandbreite zur Verfügung zu stellen. **Doch Vorsicht:** Nur einen RDP-Server ins Netz zu stellen, kann zur Falle werden. Viele Sicherheitsvorfälle aus der jüngeren Vergangenheit lassen sich auf unzureichend abgesicherte RDP-Server zurückführen. **Ideal wäre in diesem Fall eine Kombination aus RDP und VPN.** So muss ein Mitarbeiter sich zunächst mit einem Unternehmens-VPN verbinden, um schließlich auf den Terminalserver zu kommen.

 **Verwenden Sie eine sichere Chat-Umgebung für den nonverbalen Austausch der Kollegen.** Idealerweise sollte hier eine Ende-zu-Ende-Verschlüsselung zum Einsatz kommen. Viele Chat-Umgebungen lassen außerdem den sicheren Austausch von Dateien zu.

Sechs Tipps für die Zeit nach der Krise.





Jetzt lesen

So klappt's mit dem sicheren Homeoffice

Aktuelle Ereignisse
rund um IT-Sicherheit
in unserem Blog.

gdata.de/blog

Für Mitarbeiter im Homeoffice gilt:

-  Auch wenn Sie zu Hause in den eigenen vier Wänden sitzen: Sie sind mit dem Firmennetz verbunden. Daher gelten auch hier die gleichen Regeln wie für die Arbeit im Büro: **Keine unbekanntem Wechselmedien anschließen, keine verdächtigen Links anklicken, Rechner beim Verlassen sperren und Vorsicht beim Öffnen von Mailanhängen walten lassen.** Denn Phishing-Mails kommen auch dann im Postfach an, wenn Sie zu Hause arbeiten.
-  **Sorgen Sie nach Möglichkeit für eine Umgebung ohne Ablenkungen und Unterbrechungen.** Partner, Kinder oder Haustiere sollten Sie in Ruhe lassen – um so besser, wenn ein eigenes Arbeitszimmer vorhanden ist.
-  Wenn es sich vermeiden lässt: **Übertragen Sie keine größeren Dateimengen ins Firmennetz oder aus dem Firmennetz heraus.** Das hält die Auslastung für das Firmen-VPN auf einem erträglichen Maß und verhindert, dass die Verbindung für andere Mitarbeiter ausgebremst wird.
-  Wenn Sie am Geschehen in den Sozialen Medien teilnehmen und „Homeoffice-Bilder“ posten: **Achten Sie darauf, dass keine persönlichen Informationen oder Firmendaten auf Fotos zu sehen sind** (zum Beispiel E-Mails, geöffnete Dokumente etc.).



gdata.de/business

kontakt@gdata.de | +49 234 9762-170



TRUST IN
GERMAN
SICHERHEIT