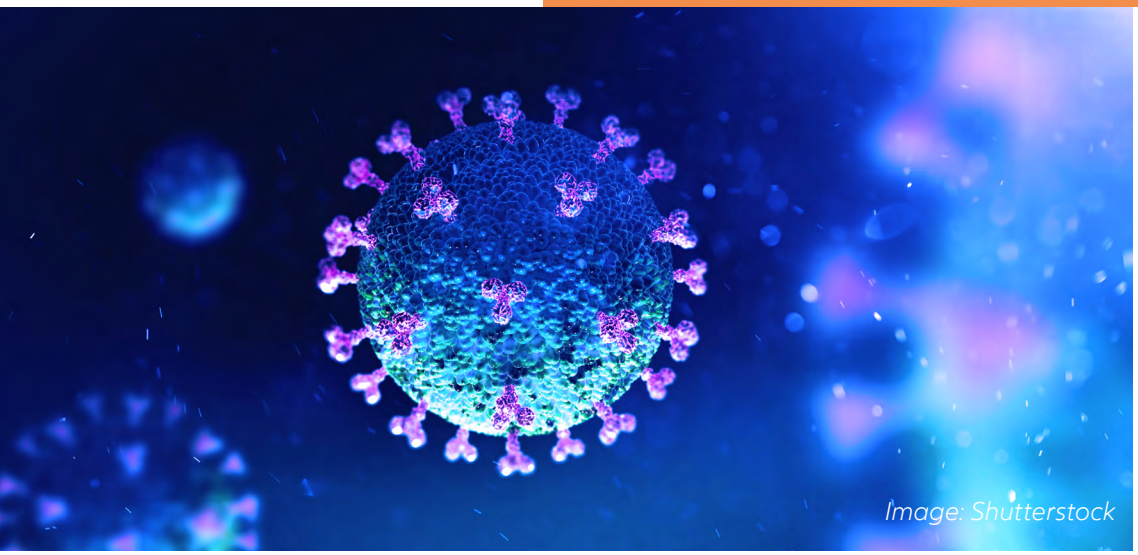
ALLIANZ GLOBAL CORPORATE & SPECIALTY®

CORONAVIRUS: CYBER-SICHER DURCH DIE PANDEMIE

ALLIANZ RISK CONSULTING



Seit dem Ausbruch des Coronavirus arbeiten viele Menschen im Home-Office. Dadurch nimmt auch die Zahl der Cyber-Vorfälle zu. Hacker, Betrüger und Spammer versuchen, Schwachstellen auszunutzen, um wertvolle Informationen zu stehlen. Als Reaktion darauf heben die AGCS-Experten eine Reihe von Maßnahmen hervor, die den Mitarbeitern helfen können, die Cyber-Herausforderungen, die Covid-19 für das Home-Office mit sich bringt, besser zu bekämpfen.

Der Coronavirus verändert die Art und Weise, wie Menschen täglich arbeiten und interagieren. Viele Unternehmen mussten infolge des Ausbruchs ihre Remote-Arbeitskapazitäten erweitern - und das meist sehr kurzfristig. Um so vielen Mitarbeitern wie möglich einen einfachen und schnellen Zugang zu Betriebssoftware und -systemen zu ermöglichen, mussten in einigen Fällen die IT-Sicherheitsstandards gesenkt oder ausgesetzt werden, was für die Unternehmen potentielle Gefahren für die Cybersicherheit mit sich brachte.

Eine Folge potenziell nachlässiger Sicherheit könnte sein, dass es Cyberkriminellen und Hackern leichter fällt, in zuvor effektiv geschützte Unternehmenssysteme einzudringen, was zu Datenverletzungen, Cyber-Erpressungen und IT-Systemausfällen führen könnte.

Leider ist der Heimarbeiter, der über eine VPN-Verbindung (Virtual Private Network) auf das Unternehmensnetzwerk zugreift, ein begehrtes Ziel für Cyberkriminelle. Die jüngsten Ereignisse zeigen dies nur zu deutlich.

Coronavirus-Phishing-Mails mit bösartigen Links oder Anhängen, die per E-Mail oder WhatsApp-Nachrichten verschickt werden, sind seit Januar 2020 im Umlauf und haben sich seitdem vermehrt. Die Europäische Kommission verzeichnet seit Beginn des Ausbruchs eine Zunahme der Cyberkriminalität. Auch die Weltgesundheitsorganisation (WHO) warnte kürzlich vor verdächtigen E-Mail-Nachrichten, mit denen versucht wird, den Covid-19-Notstand auszunutzen. In einigen Ländern zeigen Statistiken, dass die Zahl der versuchten Cyber-Angriffe zwischen Mitte Februar und Mitte März um das Fünffache gestiegen ist.

„Nur weil wir im Home-Office casual gekleidet sind, heißt das nicht, dass wir auch casual mit IT-Technik und Sicherheitstandards umgehen dürfen", sagt Jens Krickhahn, Practice Leader Cyber Insurance, AGCS Central and Eastern Europe.

Allianz

Gewisse IT-Sicherheitsstandards sind Voraussetzung für den Abschluss einer Cyberversicherung. Deshalb geben wir hier Tipps und Empfehlungen, die sich an den Kernmaßnahmen des Bundesamts für Sicherheit in der Informationstechnologie zur Absicherung gegen Angriffe aus dem Internet orientieren sowie auch an den Hinweisen der Charter of Trust, einem Zusammenschluss von Unternehmen zur Förderung der weltweiten IT-Sicherheit.

Die im folgenden gelisteten Tipps und Vorsorgemaßnahmen sind ausschließlich technischer Art und können einen Beitrag zur Risiko- und Schadensminderung leisten. Sie sind jedoch weder allgemeingültig, noch als vollständig zu verstehen und sollten im Einzelfall auf ihre Eignung geprüft und gegebenenfalls angepasst werden. Sollten Sie Fragen zum Versicherungsschutz haben, wenden Sie sich bitte an Ihren Versicherungsvermittler oder Ihren AGCS Ansprechpartner.

KERNMASSNAHMEN ZUR IT-SICHERHEIT IM HOME OFFICE

SOFTWARE AKTUELL HALTEN

Prüfen Sie, ob Sie eine aktuelle Version des Betriebssystems und der von Ihnen installierten Programme verwenden können. Prüfen Sie, ob Sie die Funktion zur automatischen Aktualisierung nutzen können, die oft die Standardeinstellung ist. Prüfen Sie ob, Sie andernfalls die Sicherheitsupdates für Ihre Software einspielen können, insbesondere für Ihren Webbrowser und Ihr Betriebssystem.

VIRENSCHUTZ UND FIREWALLS NUTZEN

Prüfen Sie, ob Sie Virenschutz und Firewalls nutzen können. Bedenken Sie aber, dass diese Maßnahme nur begleitend wirksam sein kann. Ihr Einsatz macht aber die im Folgenden genannten Tipps nicht hinfällig.

UNTERSCHIEDLICHE BENUTZERKONTEN ANLEGEN

Schadprogramme haben die gleichen Rechte auf dem PC wie das Benutzerkonto, über das sie auf den Rechner gelangt sind. Daher sollten Sie nur dann mit Administratorrechten arbeiten, wenn es unbedingt erforderlich ist.

SEIEN SIE ZURÜCKHALTEND MIT DER WEITERGABE PERSÖNLICHER DATEN

Online-Betrüger steigern ihre Erfolgsraten, indem sie ihre Opfer individuell ansprechen: Zuvor ausspionierte Daten, wie etwa Surfgewohnheiten oder Namen aus dem persönlichen Umfeld, werden dazu genutzt, Vertrauen zu erwecken. Persönliche Daten gelten heute als Währung im Netz und so werden sie auch gehandelt. Nutzen Sie in öffentlichen WLAN-Hotspots nach Möglichkeit ein mit Ihrem Heimnetz verbundenes VPN (Virtuelles Privates Netzwerk), da sonst unverschlüsselt übertragene Daten von Dritten mitgelesen werden können. Gleichzeitig schützt ein VPN auch vor einer Reihe weiterer Angriffe auf Ihren Rechner und die darauf gespeicherten Daten.

ERGÄNZENDE MASSNAHMEN ZUR IT-SICHERHEIT IM HOME OFFICE

NEHMEN SIE NUR DIE GERÄTE UND INFORMATIONEN MIT NACH HAUSE, DIE ABSOLUT NOTWENDIG SIND.

Der beste Weg, Informationen oder Geräte vor Verlust zu schützen, besteht darin, sie erst gar nicht aus ihrer gewohnten Unternehmensumgebung zu entfernen. Auf diese Weise gehen sie weder beim Transport noch bei Ihnen zu Hause verloren. Stellen Sie also sicher, dass Sie nur die Geräte und Informationen mit nach Hause nehmen, die Sie wirklich benötigen.

VERWENDEN SIE AKTUELLE WEBBROWSER

Bitte prüfen Sie, ob sie Komponenten und Plug-Ins in den Einstellungen deaktivieren können. Tragen Sie die Adressen für besonders sicherheitskritische Webseiten, etwa für das Onlinebanking, zunächst von Hand in die Adresszeile des Browsers ein und speichern Sie die so eingegebene Adresse als Lesezeichen, das Sie ab dann für den sicheren Zugang nutzen.

NUTZEN SIE UNTERSCHIEDLICHE PASSWÖRTER, DIE SIE BEI BEDARF ÄNDERN

Bewahren Sie alle Passwörter und Benutzernamen sicher auf und ändern Sie schnellstmöglich alle Passwörter, die in falsche Hände geraten sein könnten. Verwenden Sie unterschiedliche, nicht erratbare Passwörter für die verschiedenen Anwendungen und ändern Sie die von den Herstellern voreingestellten Passwörter vor der ersten Nutzung. Es ist wichtig, dass Sie sich ein Passwort gut merken können. Grundsätzlich gilt: Je länger, desto besser. Das Passwort sollte mindestens acht Zeichen lang sein, nicht im Wörterbuch vorkommen und aus Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern bestehen.

ZWEI-FAKTOR-AUTHENTISIERUNG

Dort, wo eine Zwei-Faktor-Authentisierung angeboten wird, können Sie damit den Zugang zu Ihrem Account absichern. Ein Passwortmanager kann die Handhabung unterschiedlicher Passwörter erleichtern. Geben Sie Ihre Passwörter nicht an Dritte weiter.

SCHÜTZEN SIE IHRE DATEN DURCH VERSCHLÜSSELUNG

Schützen Sie Ihre vertraulichen E-Mails mit Verschlüsselung. Wenn Sie Wireless LAN (WLAN) nutzen, achten Sie hier besonders auf die Verschlüsselung des Funknetzes. Wählen Sie in Abstimmung mit dem Information Security Richtlinien Ihres Unternehmens in Ihrem Router den Verschlüsselungsstandard WPA3 oder, wenn dieser noch nicht unterstützt wird, bis auf Weiteres WPA2. Auch hier sind die Information Security Richtlinien Ihres Unternehmens massgeblich. Wählen Sie ein komplexes, mindestens 20 Zeichen langes Passwort.

LADEN SIE DATEN NUR AUS VERTRAUENSWÜRDIGEN QUELLEN HERUNTER

Seien Sie vorsichtig, wenn Sie etwas aus dem Internet herunterladen. Vergewissern Sie sich vor dem Download von Programmen, ob die Quelle vertrauenswürdig ist. Nutzen Sie nach Möglichkeit die Webseite des jeweiligen Herstellers zum Download.

FERTIGEN SIE REGELMÄSSIG SICHERHEITSKOPIEN AN

Kommt es trotz aller Schutzmaßnahmen zu einer Infektion des PCs, können wichtige Daten verloren gehen. Um den Schaden möglichst gering zu halten, sollte geprüft werden, ob regelmäßig Sicherungskopien Ihrer Dateien auf externen Festplatten, USB-Sticks oder DVD erstellt werden können.

SCHALTEN SIE SPRACHGESTEUERTE INTELLIGENTE GERÄTE AN IHREM HEIMARBEITSPLATZ AUS UND DECKEN SIE DIE WEBCAM AB, WENN SIE SIE NICHT BENUTZEN.

Sprachassistenten hören das, was im Raum gesagt wird, und übertragen es an den Anbieter. Es kann nicht ausgeschlossen werden, dass diese Aufnahmen in die falschen Hände gelangen. Und achten Sie darauf, dass Sie die Webcam an Ihrem PC abdecken, wenn Sie sie nicht benutzen, und seien Sie vorsichtig, was Sie über die Videofunktion austauschen.

VERMISCHEN SIE NICHT DIE PERSÖNLICHE UND GESCHÄFTLICHE NUTZUNG DER GERÄTE

Machen Sie eine klare Unterscheidung zwischen Geräten und Informationen für den geschäftlichen und privaten Gebrauch und übertragen Sie keine Arbeitsdaten auf persönliche Geräte. Dadurch wird ein unbeabsichtigter Abfluss von Informationen verhindert. Als Nebeneffekt hilft es auch, die Zeit, in der Sie "bei der Arbeit" sind, von der Zeit, in der Sie "zu Hause" sind, psychologisch zu trennen.

IDENTIFIZIERUNG ALLE TEILNEHMER AN ONLINE-SITZUNGEN

Besonders leicht schleichen sich Unbefugte, die sich die Einwahldaten beschafft haben, in große Online-Meetings mit vielen Teilnehmern ein. Deshalb muss sich jeder, der in der Besprechungssoftware angezeigt wird, kurz identifizieren, besonders wenn Sie sensible Themen diskutieren und Präsentationen auf dem Bildschirm austauschen.

MELDEN SIE SICH AB, WENN SIE IHRE GERÄTE NICHT MEHR BENUTZEN, UND BEWAHREN SIE SIE SICHER AUF

Selbst wenn Sie nur eine kurze Pause machen, sperren Sie den Bildschirm Ihres PCs und Ihrer mobilen Geräte wie bei der Arbeit, damit sie während Ihrer Abwesenheit nicht zugänglich sind. Und natürlich müssen Sie auch die Geräte selbst gegen unbefugte Benutzung oder sogar Diebstahl schützen, wenn sie bei Ihnen zu Hause sind.

BEACHTEN SIE AUCH ZU HAUSE DIE SICHERHEITSPRAKTIKEN BEIM DRUCKEN UND BEI VERTRAULICHEN DOKUMENTE.

Halten Sie Ihren Schreibtisch frei von vertraulichen Dokumenten. Sperren Sie vertrauliche Dokumente in einem Schrank, wenn Sie sie nicht benötigen. Bitte entsorgen Sie keine internen oder vertraulichen Dokumente in Ihrem normalen Abfallkorb: Schreddern Sie interne oder vertrauliche Dokumente, bevor Sie sie entsorgen. Bitte prüfen Sie, ob Sie diese gefahrlos zur sicheren Entsorgung zurück ins Büro bringen können.

SEIEN SIE ÄUSSERST VORSICHTIG BEI VERDÄCHTIGEN E-MAILS ODER ANHÄNGEN, INSBESONDERE WENN SIE DEN ABSENDER NICHT KENNEN.

Besonders in der gewohnten Umgebung Ihres Heimarbeitsplatzes müssen Sie sich vor verdächtigen E-Mails in Acht nehmen. Lassen Sie sich zudem nicht durch E-Mails von unbekannten Absendern unter Druck setzen, in denen Sie zu sofortigem Handeln aufgefordert werden oder die sich beispielsweise auf die aktuelle COVID-19-Krise beziehen. Nehmen Sie sich Zeit und prüfen Sie jede E-Mail gründlich, bevor Sie sie öffnen.

WEITERE INFOS ERHALTEN SIE HIER*

https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/Empfehlungen_mobiles_Arbeiten_180320.html

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.pdf?__blob=publicationFile&v=9

CONTACTS

Jens Krickhahn
Practice Leader, Cyber Insurance, AGCS CEE
jens.krickhahn@allianz.com

Michael Daum
Senior Underwriter, Cyber Insurance AGCS CEE
michael.daum@allianz.com

Design: Graphic Design Centre

Allianz Global Corporate & Specialty SE, Fritz-Schäffer-Strasse 9, 81737 Munich, Germany

Commercial Register: Munich, HRB 208312