IT Sicherheit in der Verwaltung

1. WARUM IST IT-SICHERHEIT SO WICHTIG?

Mittlerweile ist fast jede Ebene des Alltags digitalisiert. Datenverarbeitung und Datenaustausch, Kommunikation, Prozesssteuerung – all das läuft über IT-Systeme. Und gerade deshalb ist jeder gefordert, Vorsichtsmaßnahmen für den Umgang mit diesen Systemen zu verinnerlichen wie beispielsweise die Verkehrsregeln und sich ein breites Wissen anzueignen. Denn bei umfassender Betrachtung des Themas IT-Sicherheit geht es immer auch um die Schwachstelle Mensch. Das Öffnen von Malware, etwa schädlichen Anhängen oder Links in einer E-Mail, ist der häufigste Türöffner für erfolgreiche Cyberangriffe. Unerlässlich sind deshalb auch Schulungen, die Mitarbeiter für das Thema IT-Security sensibilisieren und darüber aufklären, wie sehr sich die Branche Cyberkriminalität professionalisiert hat und wie Cyberangriffe ablaufen. Wichtig ist neben dem Wissensaufbau und der Etablierung konkreter Prozesse auch eine strategische Herangehensweise, um der Bedrohungslage wirklich Herr zu werden.
Wenn es um den Schutz und die Sicherheit von Daten geht, vertrauen die Bürgerinnen und Bürger den Behörden und Institutionen der öffentlichen Hand. Umso wichtiger ist, dass dieses Vertrauen nicht enttäuscht wird und Prozesse, die den Alltag von Millionen Bürgern direkt beeinflussen, möglichst reibungslos und fehlerfrei ablaufen. Mit jedem Vorfall gehen Reputation und Vertrauen verloren, das beeinträchtigt nicht nur die betroffene Behörde, sondern den öffentlichen Sektor allgemein.

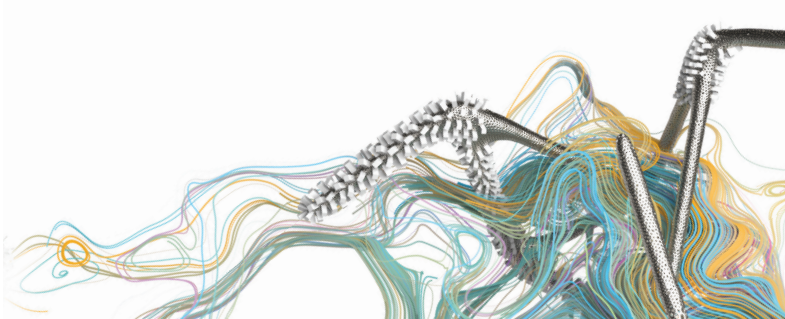
2. WAS GENAU VERSTEHT MAN UNTER IT-SICHERHEIT?

Unter dem Begriff IT-Sicherheit sind Ansätze, Prozesse, Maßnahmen und technische Werkzeuge zusammengefasst, die eingesetzt werden, um die IT-Infrastruktur vor Gefahren zu schützen. Dazu gehören Daten und Netzwerke, Geräte und Anwendungen, aber auch die Anwender. Konkrete Beispiele sind Zugriffskontrollen, Rechtemanagement, Firewalls, Virenscanner, Vulnerability Management und Proxys.

3. WIE KRITISCH IST DIE LAGE?

Die Bedrohungslage ist ernst. Cyberkriminelle und Cyberterroristen sind hocheffektiv und professionell. Sie werden ständig schneller und versierter, und ihre Methoden werden gefährlicher. So hat das BSI beispielsweise für Herbst/Winter 2020 festgestellt, dass überdurchschnittlich viele neue Varianten von Schadprogrammen aufkamen (der Tageszuwachs lag zeitweise bei knapp 470.000 Varianten). Zugleich erreichte 2019/2020 die Bedrohung durch Daten-Leaks eine neue Qualität, zum Beispiel mit der Offenlegung von Millionen von Patientendatensätzen im Internet. Unter anderem tauchten Datenbanken mit hochsensiblen medizinischen Daten frei zugänglich im Internet auf. Anders als bei Datendiebstählen war in diesem Fall kein technisch aufwendiger Angriff notwendig – die Ursache für den Datenabfluss waren unzureichend gesicherte oder falsch konfigurierte Datenbanken.

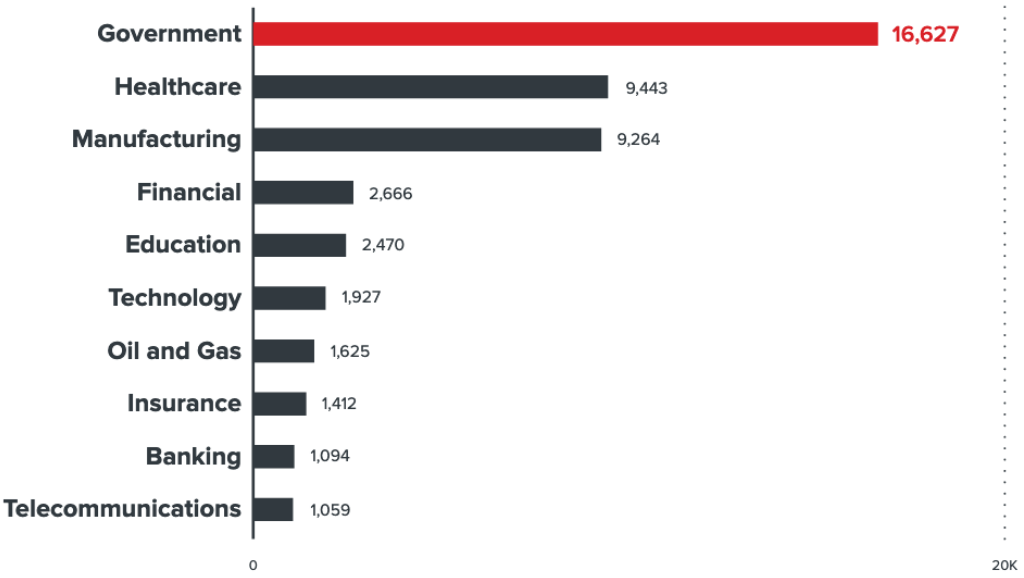
Das Bundesministerium des Innern sieht in der Nachhaltigkeit und Zielauswahl von Cyberangriffen deutlich den Versuch, die Politik und Verwaltung in Deutschland strategisch auszuspionieren.
Angriffe bedeuten für die zuständigen Institutionen einen Kontrollverlust, Kosten durch Ausfälle, Wartungskosten oder Erpressung, die Unterbrechung von Prozessen und Projekten mit langfristigen Auswirkungen, außerdem negative Folgen für die Reputation. Auch wenn nur einzelne Institutionen vom Netz genommen und in ihrer Handlungsfähigkeit eingeschränkt werden oder Daten verlieren, kann dies massive Auswirkungen haben. Ein Beispiel ist die Test-, Datensammlungs- und Impflogistik im Zusammenhang mit der Corona-Pandemie. Hier wird deutlich, wie sensibel die Gesamtlage ist.



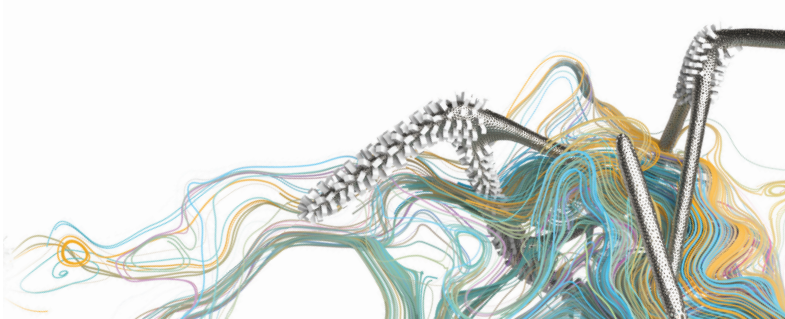
Exkurs: Aktuelle Bedrohungslage – die Auswirkungen der Corona Pandemie

Was sich früh im Jahr 2020 prognostizieren ließ: Die Corona-Pandemie hat die Cybersicherheitslage in Deutschland nachhaltig verändert. Noch mehr Prozesse und Kommunikation als bisher finden digital statt, und diejenigen, die Schaden anrichten wollen, sind sich der Sensibilität der Lage voll bewusst. Nie zuvor hing das gesellschaftliche Leben so sehr davon ab, dass die digitale Infrastruktur funktioniert – und genau das macht die Situation so prekär. Oft wurden die Krise und die damit verbundene Verunsicherung als Aufhänger für Angriffe verwendet. So gab es beispielsweise präparierte E-Mails mit vermeintlichen Impfregistrierungen oder Informationen zum Tragen von Schutzmasken.

In einem Sicherheitsüberblick zur Jahresmitte 2020 befasst sich Trend Micro eingehend mit den Herausforderungen in Zeiten der Pandemie. Dabei geht es vor allem um Bedrohungen in Zusammenhang mit COVID-19 und um gezielte Ransomware-Angriffe. Der Behördensektor war am häufigsten von solchen Angriffen betroffen.



Quelle: The top targeted identified industries based on ransomware file detections in the first half of 2020 Source: Trend Micro Smart Protection Network infrastructure (Figure 16/ P. 20, Schutz für Ihren Arbeitsplatz in Zeiten der Pandemie: Trend Micro Cybersicherheitsbericht zur Jahresmitte 2020 - S



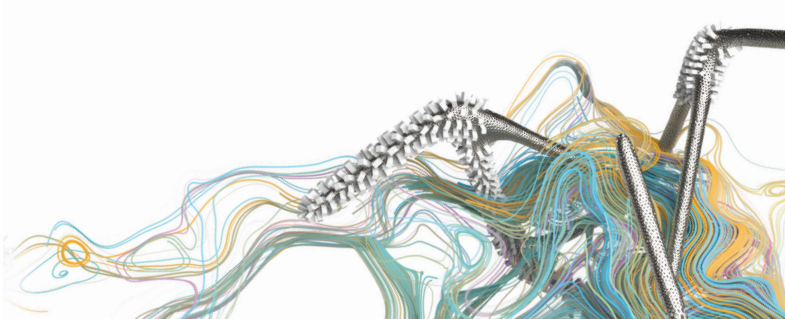
Dies lässt sich auch in der täglichen Arbeit erkennen: Die Bedrohungslage ist real, und Cyberangriffe sind alltäglich. Im ersten Halbjahr 2020 konnte Trend Micro mithilfe eines entsprechenden Tools über 27 Milliarden Bedrohungen blocken. Eine Übersicht der blockierten E-Mail-Bedrohungen, schädlichen Dateien und schädlichen URLs zeigt die folgende Grafik:

Quelle: Schutz für Ihren Arbeitsplatz in Zeiten der Pandemie: Trend Micro Cybersicherheitsbericht zur Jahresmitte 2020 - Security Roundup - Trend Micro DE

4. WAS KANN PASSIEREN?

Die Verfügbarkeit von Systemen kann beeinträchtigt sein – bis hin zum Komplettausfall. Dies ist besonders problematisch, wenn es kritische Infrastrukturen betrifft, aber auch kleinere Vorfälle können die Abläufe in der öffentlichen Verwaltung signifikant stören. Beispiele sind:

- Vireninfektion oder störende Software
- Missbrauch der Informationssysteme durch Mitarbeiter
- Zugriff von Außenstehenden (einschließlich Hacker-Angriffe)
- Diebstahl oder Betrug mithilfe von Computern
- Diebstahl oder unbefugte Weitergabe vertraulicher Daten
- Erpressung durch sogenannte Ransomware



5. WELCHE FALLSTRICKE GIBT ES BEI DER PLANUNG UND IMPLEMENTIERUNG VON MASSNAHMEN IM BEREICH DER IT-SICHERHEIT?

Investitionen lohnen sich, und Stückwerk führt schnell zu Schutzlücken, zum Beispiel wenn verschiedene Lösungen punktuell an unterschiedlichen Stellen und unkoordiniert eingesetzt werden. Generell funktioniert eine Schutzinfrastruktur nur auf Basis einer fundierten Strategie. Idealerweise ist ein System so strukturiert, dass es Gefahren frühzeitig identifiziert (Feuermelder) und nicht nur auf akute Gefahren reagiert (Feuerwehr). Das muss vor allem in die Budgetplanung einfließen. Ein ganzheitlicher, systemischer Ansatz, der über alle Schnittstellen und Ebenen hinweg funktioniert wie eine gut geölte Maschine, Gefahren signifikant minimiert und Synergieeffekte schafft, ist eine Investition, die sich auszahlt.
Die Gelder, die in die IT-Sicherheit fließen, sind also keine lästige Ausgabe, sondern eine notwendige und sinnvolle Investition. Denn die Kosten eines Cybersicherheitsvorfalls übersteigen meist bei Weitem die Investitionen in notwendige IT-Sicherheitstechnologie. Zu den Kosten für die Schadensermittlung, die Wiederherstellung und gegebenenfalls neue Hardwarekomponenten können weitere hinzukommen, etwa Rechtsberatungskosten, mögliche Strafen und Bußgelder, Zahlungen im Zusammenhang mit Erpressungen durch Ransomware, Ausgaben für Krisenmanagement und -kommunikation. Nicht konkret zu beziffern ist der Reputationsschaden, der vor allem mit Blick auf die Rolle und Aufgaben der öffentlichen Verwaltung ein folgenschwer sein kann.

6. WIE SIEHT EINE ERFOLGREICHE HERANGEHENSWEISE AUS?

Für die Lösung von Sicherheitsfragen gibt es kein Patentrezept. Angreifer nutzen heute modernste Technologien, zum Beispiel Künstliche Intelligenz. Nur mit dem Einsatz ebensolcher modernen Technologien ist diesen Angriffen effektiv beizukommen. Es geht darum, dem Angreifer immer einen Schritt voraus zu sein. Dies erfordert einen intelligenten, mehrschichtigen Ansatz, in dessen Zentrum die Automatisierung der IT-Sicherheit steht. Durch ein ähnlich schnelles und agiles Vorgehen, wie es der Angreifer selbst an den Tag legt, lassen sich menschliche Fehler weitestgehend ausschließen.

7. WELCHE SIND DIE WICHTIGSTEN KONKRETEN MASSNAHMEN?

E-Mail-Bedrohungen eindämmen: E-Mail ist heute der Angriffsvektor Nummer eins, 94 % aller Angriffe starten mit einer Mail. Es ist deshalb wichtig, in diesem Bereich zu investieren. Standard-Virenscanner sind nicht in der Lage, diese Bedrohungen zu erkennen. Sie müssen nach dem Stand der Technik mit Testsystemen für eingehende Mails verstärkt werden. In diesen Testsystemen (Sandboxing) wird jede hochverdächtige E-Mail auf ihre Auswirkungen beim Öffnen getestet – bevor sie empfangen werden kann. Es wird also simuliert, was passiert, wenn ein Mitarbeiter die Mail öffnet.

Virenschutz: Die üblichen Virenscanner sind aktuellen Bedrohungen nicht gewachsen. Ein moderner Virenschutz muss deshalb auf Techniken wie Maschinelles Lernen und Verhaltenskontrolle bauen. Maschinelles Lernen macht es möglich, die zu prüfenden Dateien auf bestimmte Muster zu untersuchen und mit bereits bekannten Viren zu vergleichen. Die Verhaltenskontrolle prüft zum Beispiel, ob sich eine Textdatei so verhält, wie es eine Textdatei normalerweise tut. Treten Abweichungen auf, führt dies zu entsprechenden Blockierungs- und Alarmaktionen.

Netze schützen: Die bestehende Firewall verhindert den unbefugten Zugriff auf das Netzwerk. Ein Intrusion Detection System überwacht die Netzwerkaktivität, sucht nach bösartigem oder anormalem Verhalten, reagiert darauf und stoppt es. Dieses System durchleuchtet also den gesamten Datenstrom bis in die Tiefe und sucht nach Angriffsmustern.

Schwachstellen vermeiden: Schwachstellen sind meist offene Angriffsflächen, die durch Computer oder Server entstehen, die nicht immer auf dem aktuellen Stand der Software-Updates sind. Diese Updates werden oft zu spät eingespielt, oder es gibt noch keine. Eine Sonderform stellen dabei Zero-Day-Bedrohungen dar: Angriffe, die bisher unbekannte Schwachstellen ausnutzen und für die der Hersteller noch keinen Patch verteilen kann.

Stand der Technik ist heute, Netzwerke durch ein Intrusion Prevention System zu schützen. Durch den Einsatz von Systemen, die ähnlich schnell und flexibel agieren wie die Angreifer und die durch die Antizipation von möglichen Angriffsszenarien schneller eine Versiegelung für die Lücke zur Verfügung stellen können, lassen sich entsprechende Gefahren deutlich eindämmen.
Im Jahr 2020 wurden beispielsweise empfindliche Systeme wie MS-Exchange-Server angegriffen, weil notwendige Patches nicht verfügbar bzw. nicht aktiviert waren.

Daten schützen: Oft gehen sensible Daten verloren, wenn Informationen auf einen USB-Stick oder in einen Cloud-Speicher kopiert, per E-Mail versendet oder anderweitig weitergereicht werden. Data Loss Prevention schafft Abhilfe. Die Lösung untersucht den gesamten Datenverkehr, der aus dem Behördennetzwerk fließt, auf Daten, die in einer Richtlinie definiert wurden. Das System sucht also nach frei definierbaren Merkmalen in Dokumenten, etwa nach Wörtern (vertraulich, VS-NFD, Nummern) oder Wasserzeichen. Tauchen diese in Dokumenten auf, wird das Ausleiten dieser Daten blockiert. Die Kontrollinstanz befindet sich dabei oft auf Mailservern, Internetknoten oder auf dem Computer des Mitarbeiters selbst.

Selbstverteidigungssystem einsetzen: Moderne IT-Sicherheitslösungen innerhalb einer Behörde müssen miteinander vernetzt sei. Dies ermöglicht den ständigen Austausch von Bedrohungsinformationen und schafft die Basis dafür, sich ständig automatisch auf neue Angriffsvarianten einzustellen. So informiert das Internetgateway beispielsweise alle Computer vorab, wenn eine neue Bedrohung ins Netzwerk eingedrungen ist, und alle anderen Systeme stellen sich automatisch auf die Bekämpfung dieser Bedrohung ein.

8. WAS TUN, WENN ES ZU EINEM VORFALL KAM?

Nach einem Angriff muss es vorrangig darum gehen, den Schaden einzudämmen und das System schnell wieder zum Laufen zu bringen. Dazu gehört die Identifizierung und Qualifizierung der Bedrohung. Ein Vorfall zeigt immer, dass die Präventivmechanismen versagt haben und verstärkt werden müssen.

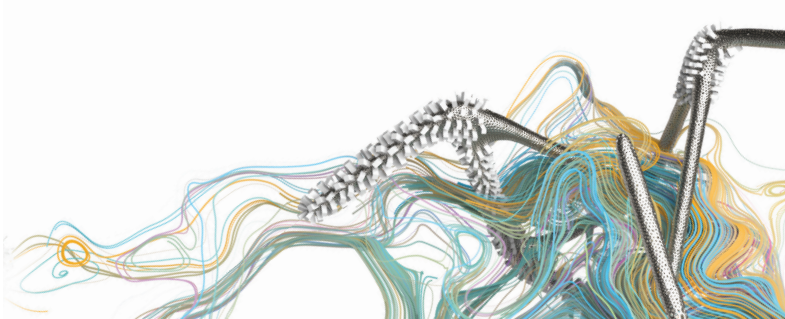
Folgende Schritte tragen zu einer optimalen Problemlösung bei:

Vorbereitung: Notwendig sind Richtlinien und Protokolle, die im Falle eines Angriffs zu befolgen sind. Diese Protokolle müssen unter anderem eine Liste der Personen und Stellen enthalten, die im Falle eines Verstoßes informiert werden müssen. Erkennung, Identifizierung und Analyse erfordern zeitgemäße Werkzeuge, die dazu dienen, Bedrohungen zu erkennen und Endpunkte, Netzwerkverkehr und andere Datenquellen zu überwachen. Auf diesem Wege lässt sich eine fundierte Einschätzung der Situation treffen, auf deren Grundlage weitere Maßnahmen ergriffen werden können.

Isolieren: Die betroffenen Systeme müssen über die Netzwerkzugriffskontrolle vom Netzwerk isoliert werden. Das bedeutet aber nicht, dass das System ausgeschaltet wird. Bestimmte Informationen müssen eventuell für weitere Untersuchungen zur Verfügung stehen.

Extraktion: Die Bedrohung muss aus dem System entfernt und zur weiteren Analyse einem Sicherheitsexperten oder einem Sicherheitsanbieter übergeben werden.

Ergänzend: Moderne Incident-Response-Werkzeuge zeichnen sich dadurch aus, dass sie erfolgreich sein können, ohne den Bedrohungsakteur hinter dem Angriff identifizieren zu müssen. Incident Response geschieht live, also während eines laufenden Angriffs, mit der Absicht, diesen zu stoppen.



Anlage: Die wichtigsten Begriffe im Überblick

Bot: Trojaner, der mit dem Internet verbundene Computer und Geräte so infiziert, dass sie ein Angreifer fernsteuern kann. Ein Botnet ist demzufolge ein Netzwerk aus gekaperten Computern und Geräten, die mit Bot-Malware infiziert sind und von einem Hacker ferngesteuert werden.

CERT: Computer Emergency Response Team

Cloud Computing: Nutzung von zum Beispiel im Internet gehosteten Servern. Die Nutzung von Cloud-Technologien kann Zeit und Geld sparen und gleichzeitig die Produktivität der Mitarbeiter steigern. Cloud-Technologien lassen sich schnell bereitstellen, erfordern minimales technisches Know-how zur Verwaltung und kosten weniger als Technologien vor Ort.

Denial of Service (DoS): Cyberangriff, der darauf abzielt, ein Netzwerk, eine Website oder einen Dienst zu deaktivieren, herunterzufahren oder zu stören. Typischerweise wird eine Malware verwendet, um den normalen Datenfluss in und aus einem System zu unterbrechen oder zu hemmen und das Ziel für einen bestimmten Zeitraum unbrauchbar oder unzugänglich zu machen.

Exploit: Code, der eine Software-Schwachstelle oder eine Sicherheitslücke ausnutzt. Exploits ermöglichen es einem Eindringling, aus der Ferne auf ein Netzwerk zuzugreifen und erhöhte Rechte zu erlangen oder tiefer in das Netzwerk einzudringen.

Firewall: System, das verhindert, dass Computer in einem Netzwerk direkt mit externen Computersystemen kommunizieren können. Eine Firewall besteht in der Regel aus einem Computer, der als Barriere fungiert. Durch diese Barriere werden alle Informationen analysiert, die zwischen den Netzwerken und den externen Systemen übertragen werden. Die Firewall-Software blockiert die Übertragung von Informationen, wenn diese nicht den vorkonfigurierten Regeln entsprechen.

Malware: allgemeiner Begriff für einen bösartigen Code, der Viren, Würmer und Trojaner umfasst

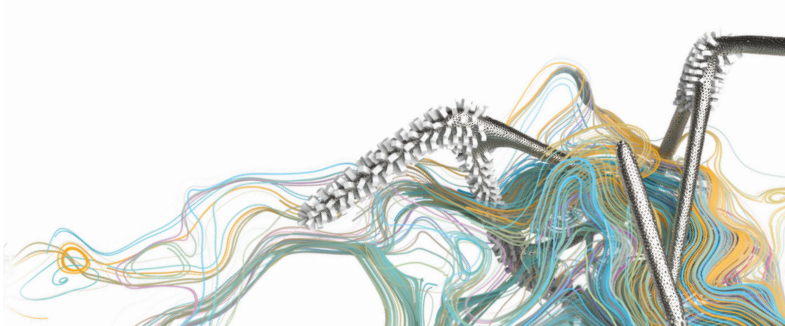
Managed Detection and Response (MDR): ausgelagerter Service, der Unternehmen mit Threat Hunting Services versorgt und auf Bedrohungen reagiert, sobald diese entdeckt werden. Sicherheitsanbieter stellen ihren MDR-Kunden zudem ihren Pool an Sicherheitsforschern und -ingenieuren zur Verfügung, die für die Überwachung von Netzwerken, die Analyse von Vorfällen und die Reaktion auf Sicherheitsfälle zuständig sind.

OZG: Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (OZG), das die Rahmenbedingungen für die Digitalisierung in der öffentlichen Verwaltung festlegt

Phishing: Form des Identitätsdiebstahls, bei der ein Betrüger eine authentisch aussehende E-Mail von einem seriösen Unternehmen verwendet, um Empfänger dazu zu bringen, vertrauliche persönliche Daten herauszugeben

Privacy by Design: Konzept, das den Datenschutz in die Entwicklung und den Betrieb von neuen Geräten, IT-Systemen, vernetzter Infrastruktur und sogar Unternehmensrichtlinien integriert. Durch die Entwicklung und Integration von Datenschutzlösungen in den frühen Phasen eines Projekts lassen sich mögliche Probleme frühzeitig erkennen und langfristig vermeiden.

Ransomware: Malware, die den Zugriff des Benutzers auf sein System verhindert oder einschränkt, bis ein Lösegeld gezahlt wird. Modernere Ransomware-Familien, die kollektiv als Krypto-Ransomware kategorisiert werden, verschlüsseln bestimmte Dateitypen auf infizierten Systemen und zwingen Benutzer dazu, über bestimmte Online-Zahlungsmethoden Lösegeld zu bezahlen, um einen Entschlüsselungsschlüssel zu erhalten.



SOC: Security Operations Center, Zentrale für alle sicherheitsrelevanten Services im IT-Umfeld von Organisationen oder Unternehmen. Das SOC schützt die IT-Infrastruktur und Daten vor internen und externen Gefahren. (Was ist ein Security Operations Center (SOC)? (security-insider.de))

Threats: Sicherheitsprobleme, zum Beispiel Malware, Grayware/Adware, Spyware, Spam, Phishing und Bots/Botnets

Virus: Computerprogramm, das sich selbst kopieren und einen Computer ohne die Erlaubnis oder das Wissen des Benutzers infizieren kann

Zero-Day-Vulnerability: allgemein unbekannte Schwachstelle in einem System oder Gerät, die Sicherheitsforscher zwar erkennen, für die Softwareentwickler aber noch keinen Patch herausgegeben haben

Über Trend Micro
Als einer der weltweit führenden Anbieter von IT-Sicherheit verfolgt Trend Micro mit Leidenschaft das Ziel, eine sichere Welt für den digitalen Datenaustausch zu schaffen – heute und in Zukunft. Unsere innovativen Lösungen für Privatanwender, Unternehmen und Behörden bieten dank der XGen™ Sicherheitsstrategie vernetzten Schutz für Rechenzentren, Cloud-Workloads, Netzwerke und Endpunkte. Unsere Connected Threat Defense ermöglicht das nahtlose Teilen von Bedrohungsinformationen und bietet zentrale Transparenz und Kontrolle, um Organisationen bestmöglich zu schützen.
Mit über 6.500 Mitarbeitern in 50 Ländern und der weltweit fortschrittlichsten Erforschung und Auswertung globaler Cyberbedrohungen bietet Trend Micro Schutz für eine vernetzte Welt.
Weitere Informationen: **www.trendmicro.com**.

Securing Your Connected World

Trend Micro Deutschland GmbH
Parkring 29
85748 Garching
www.trendmicro.com