Microsoft Security

Ransomware-as-a-Service als neues Aushängeschild der industrialisierten Cyber-Kriminalität

Handgemachte Angriffe als neuestes Geschäftsmodell beflügeln Cyber-Kriminelle aller Art.

Ransomware gehört zu den hartnäckigsten und gängigsten Cyber-Bedrohungen. Sie entwickelt sich kontinuierlich weiter und stellt in ihrer aktuellen Form für Unternehmen weltweit eine neuartige Bedrohung dar. Zur Weiterentwicklung von Ransomware bedarf es keiner technologischen Fortschritte. Stattdessen kommt ein neues Geschäftsmodell zum Tragen, nämlich Ransomware-as-a-Service (RaaS).

Ransomware-as-a-Service (RaaS) erfolgt in Zusammenarbeit zwischen einem Betreiber, der Tools zur Durchführung von Erpressungen entwickelt und pflegt, und einem Partner, der für die Ransomware-Payload zuständig ist. Gelingt dem Partner ein erfolgreicher Ransomware-Angriff mit anschließender Erpressung, profitieren beide davon.

Das RaaS-Modell senkt die Einstiegsschwelle für Angreifer, denen die technischen Kenntnisse zur Entwicklung eigener Tools fehlen, die aber sofort anwendbare Tools für Penetrationstests sowie Sysadmin zur Durchführung von Angriffen nutzen können. Technisch weniger gewiefte Täter können somit von technisch besser ausgebildeten, die bereits in einen Sicherheitsbereich eingedrungen sind, einen Netzwerkzugriff kaufen.

Obwohl RaaS-Partner sich Ransomware-Payloads zunutze machen, die von versierten Betreibern angeboten werden, gehören sie nicht zur selben Ransomware-Bande, sondern haben vielmehr ihre eigenen Cybercrime-Unternehmungen.

Mehr Möglichkeiten für Internetkriminelle, mehr Cyber-Kriminalität

Das Ransomware-as-a-Service-Modell erweitert die Möglichkeiten von Kriminellen ohne solide Computerkenntnisse schnell und deutlich. In der Vergangenheit setzten unbedarfte Täter eher selbst entwickelte oder gekaufte Malware für Angriffe in geringem Ausmaß ein. Jetzt aber können sie alles, was sie benötigen, bei einem RaaS-Betreiber zu einem gewissen Preis einkaufen – von Netzwerkzugängen bis hin zu Ransomware-Payloads. Viele RaaS-Programme enthalten zudem eine Reihe von Zusatzangeboten zur geplante Erpressung, darunter Hosting von Betrugswebsites und Einbindung in Lösegeldforderungen sowie Entschlüsselungsverhandlungen, Zahlungsdruck und Dienste zur Transaktion in Kryptowährungen.

Die Folgen eines erfolgreichen erpresserischen Ransomware-Angriffs sind also unabhängig von den technischen Kenntnissen des Angreifers gleich.

Netzwerkschwachstellen suchen und ausnutzen – zu einem gewissen Preis

Eine Möglichkeit für RaaS-Betreiber, ihren Partnern einen Mehrwert zu verschaffen, sind bereits gekaperte Netzwerkzugänge. Kriminelle, die mit manipulierten Netzwerkzugriffen handeln, suchen im Internet nach geeigneten Systemen, in die sie eindringen und die sie später ausbeuten können.

Damit Angreifer auch erfolgreich sind, brauchen sie Zugangsdaten. Gestohlene Zugangsdaten sind für diese Angriffe so wichtig, dass im Preis für einen Netzwerkzugriff oftmals ein garantiertes Administratorkonto inbegriffen ist.

Die Vorgehensweise der Täter nach Erhalt des Netzwerkzugriffs variiert mitunter stark und hängt von den einzelnen Gruppen, ihren Workloads oder ihrer Motivation ab. Die Zeit, die zwischen Erstzugriff und einer bequemen Bereitstellung mit ein paar Tastenanschlägen vergeht, schwankt daher zwischen Minuten und Tagen oder noch länger. Aber wenn die Umstände es zulassen, kann im Bruchteil einer Sekunde Schaden angerichtet werden. Tatsächlich ist zwischen Erstzugriff und kompletter Lösegeldzahlung (einschließlich Übergabe von einem Zugriffshändler an einen RaaS-Partner) eine Dauer von unter einer Stunde bekannt.

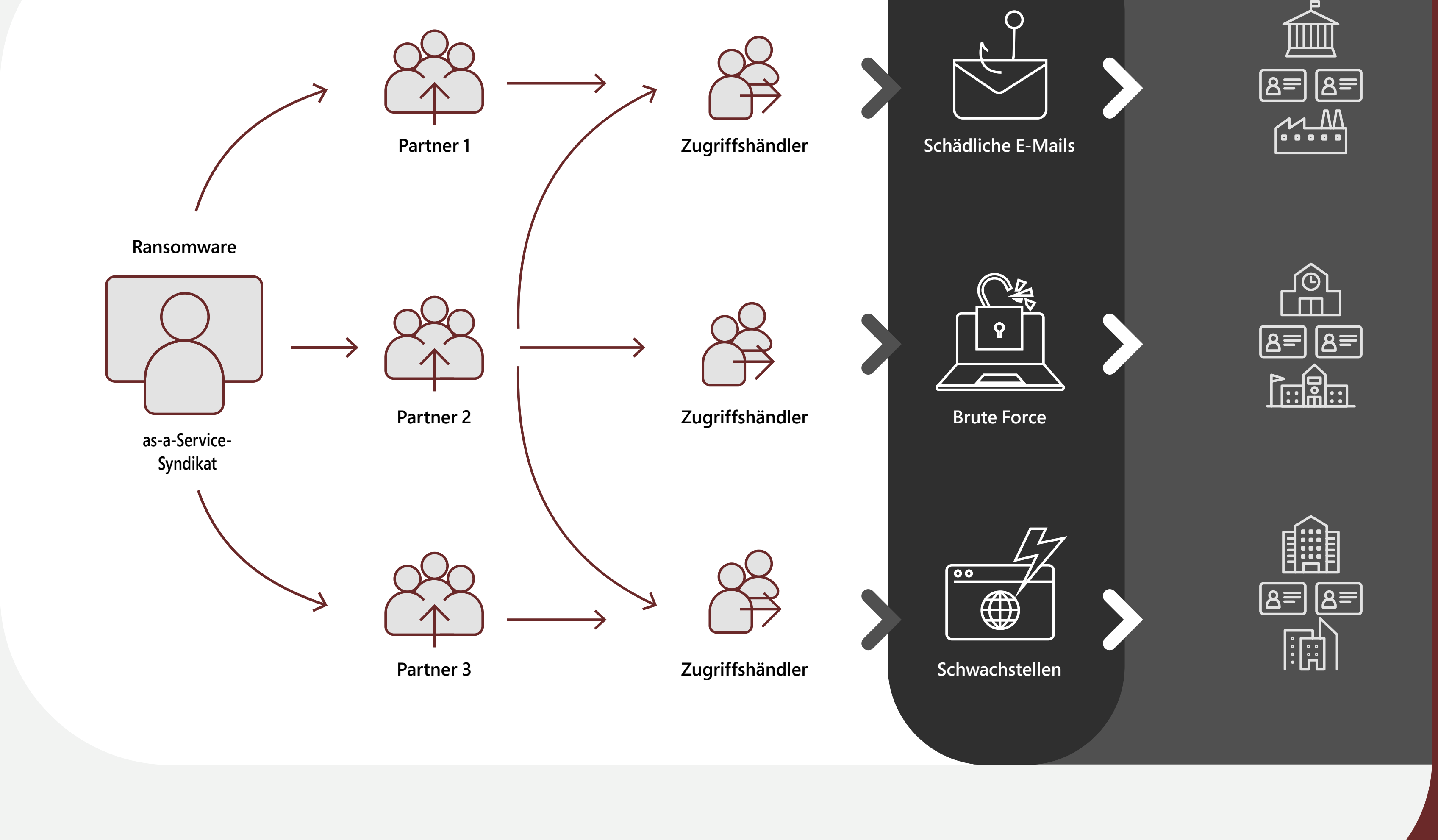
Die Wirtschaft am Laufen halten – persistente und hinterhältige Zugriffsmethoden

Sobald sich Angreifer Zugriff auf ein Netzwerk verschafft haben, bleiben sie gerne auch dann noch, nachdem das Lösegeld längt bezahlt wurde. Die Lösegeldzahlung verringert somit nicht unbedingt das Risiko, dem ein betroffenes Netzwerk ausgesetzt ist, und dient den Tätern möglicherweise nur zur Finanzierung. Sie werden das Netzwerk so lange weiter mit anderer Malware oder anderen Ransomware-Payloads angreifen und Geld erpressen, bis sie aus dem System vertrieben werden.

Die Übergabe, die zwischen verschiedenen Angreifern stattfindet, deutet darauf hin, dass in einer Umgebung mehrere Gruppen mit unterschiedlichen Vorgehensweisen aktiv sein können, die sich von den bei einem Ransomware-Angriff verwendeten Tools unterscheiden. So folgt beispielsweise auf den mit einem Onlinebanking-Trojaner verschafften Erstzugriff eine Cobalt-Strike-Bereitstellung, aber der RaaS-Partner, der den Zugriff erworben hat, kann sich entscheiden, die Aktion mit einem Fernzugriffstool wie TeamViewer durchzuführen.

Die Verwendung rechtmäßiger Tools und Einstellungen im Vergleich zu Malware-Implantaten wie Cobalt Strike ist bei Ransomware-Angreifern beliebt, um nicht entdeckt zu werden und sich länger in einem Netzwerk aufhalten zu können.

Eine weitere gängige Vorgehensweise von Angreifern ist die Erstellung neuer Backdoor-Benutzerkonten, ob lokal oder in Active Directory, die dann Fernzugriffstools wie einem virtuellen privaten Netzwerk (VPN) oder Remotedesktop hinzugefügt werden können. Von Ransomware-Angreifern ist auch bekannt, dass sie die Systemeinstellungen ändern, um Remotedesktop zu aktivieren, die Sicherheit des Protokolls zu verringern und der Remotedesktop-Benutzergruppe neue Mitglieder hinzuzufügen.



Auf Tuchfühlung mit den hinterhältigsten Gegnern der Welt, die sich nicht fassen lassen

Eine der Eigenschaften von RaaS, die es so bedenklich macht, ist, dass es von Menschen abhängt, die bewusste und überlegte Entscheidungen treffen und die Angriffsmuster entsprechend dem, was sie in den ausgesuchten Netzwerken finden, verschieden gestalten können, So wird sichergestellt wird, dass die Angreifer ihr Ziel auch erreichen.

Für diese Art von Angriffen hat Microsoft den Begriff von Menschen platzierte Ransomware geprägt, denn es handelt sich um eine Handlungskette, die letztendlich zu Ransomware-Payloads führt, und eben nicht um Malware-Payloads, die es zu blockieren gilt.

Während die meisten Aktionen im Rahmen des Erstzugriffs automatisiert ablaufen, nutzen Angreifer, sobald der Angriff in die praktische Phase übergeht, ihr Know-how, um die Sicherheitsmechanismen der attackierten Umgebung auszuschalten.

Ransomware-Angreifer haben es auf schnelles und leicht zu verdienendes Geld abgesehen. Bei der Bekämpfung dieser Art von Cyber-Kriminalität ist es daher entscheidend, die Kosten, die den Tätern entstehen, durch bessere Sicherheitsmechanismen nach oben zu treiben. Weil die Entscheidungen bei Ransomware-Angriffen von Menschen getroffen werden, verbleiben die Angreifer auch dann im Netzwerk, nachdem bestimmte Angriffsphasen von Sicherheitsprodukten erkannt wurden. Sofern die Täter nicht von einer Sicherheitskontrolle blockiert werden, werden sie es immer weiter versuchen. Erkennt ein Antivirenprogramm ein Tool oder eine Payload und blockiert diese, wechseln die Angreifer oftmals einfach das Tool oder ändern die Payload.

Angreifer kennen sich zudem mit den Reaktionszeiten von Sicherheitszentren (SOC) und dem Potenzial und den Einschränkungen von Erkennungstools aus. Sobald die Phase erreicht ist, in der Sicherungen oder Schattenkopien gelöscht werden, dauert es bis zur Ransomware-Bereitstellung nur noch wenige Minuten. Zu diesem Zeitpunkt haben die Täter sehr wahrscheinlich schon kriminelle Aktivitäten wie Datenexfiltrationen durchgeführt. Dies zu wissen, ist für Sicherheitsteams bei ihrer Reaktion auf einen Ransomware-Angriff maßgeblich: Menschliche Gegner lassen sich nur stoppen, wenn bei Feststellung einer Unregelmäßigkeit wie Cobalt Strike Untersuchungen noch vor der Phase angestellt werden, in der die Ransomware verteilt wird, und indem sofort Maßnahmen zur Schadensbegrenzung und Abwehr eingeleitet werden.

Besserer Schutz vor Bedrohungen ohne den vielen Warnhinweisen überdrüssig zu werden

Eine solide Sicherheitsstrategie zum Schutz vor abgebrühten Tätern muss Erkennungs- und Eindämmungsvorgaben beinhalten. Sich nur auf die Erkennung von Bedrohungen zu verlassen, reicht aus den folgenden zwei Gründen nicht aus: Manche Infiltrationen sind praktisch nicht zu erkennen (sie erscheinen wie mehrere harmlose Aktionen), und Ransomware-Angriffe werden aufgrund zu vieler Warnhinweise, die von verschiedenen Sicherheitsprodukten ausgegeben werden, schlichtweg übersehen.

Weil Angreifer mehrere Möglichkeiten zur Umgehung und Deaktivierung von Sicherheitsmechanismen haben und weil sie in der Lage sind, ein unauffälliges Administratorverhalten an den Tag zu legen, um so nicht weiter bemerkt zu werden, müssen IT-Sicherheitsteams ihre Erkennungsaktivitäten mit besseren Sicherheitsmaßnahmen verstärken.

Ransomware-Angreifer haben es auf schnelles und leicht zu verdienendes Geld abgesehen. Bei der Bekämpfung dieser Art von Cyber-Kriminalität ist es daher entscheidend, die Kosten, die den Tätern entstehen, durch bessere Sicherheitsmechanismen nach oben zu treiben.

Dies sind nur einige Möglichkeiten, wie Unternehmen sich besser schützen können:

Zugangsdaten pflegen:
Segmentieren Sie das Netzwerk logisch nach Berechtigungen, die neben der Netzwerksegmentierung implementiert werden können, um laterale Bewegungen einzuschränken.

Offenlegung von Zugangsdaten überwachen:
Eine Überwachung der Offenlegung von Zugangsdaten ist entscheidend bei der Verhinderung von Ransomware-Angriffen und Cyber-Kriminalität allgemein. IT-Sicherheitsteams und SOCs können zusammenarbeiten, um verwaltungstechnische Berechtigungen zu minimieren und herauszufinden, auf welcher Ebene Zugangsdaten offengelegt werden.

Cloud besser schützen:
Je mehr Cloud-Ressourcen ins Visier von Kriminellen geraten, desto wichtiger ist es, diese Ressourcen, Identitäten und lokale Konten zu schützen. Sicherheitsteams müssen die Infrastruktur zur Identitätssicherung verbessern, indem bei allen Konten Multi-Faktor-Authentifizierung (MFA) erforderlich ist und indem Cloud-Administratoren und -Mandanten in Bezug auf Sicherheit und Zugangsdatenpflege genauso behandelt werden wie Domänenadministratoren.

Sicherheitsschwachstellen beseitigen:
Unternehmen müssen dafür sorgen, dass ihre Sicherheitstools optimal konfiguriert sind. Bei regelmäßigen Netzwerkscans muss zudem sichergestellt werden, dass das Sicherheitsprodukt alle Systeme schützt.

Angriffsfläche verringern:
Erstellen Sie Regeln zur Verringerung der Angriffsfläche, um gängige Vorgehensweisen bei Ransomware-Angriffen zu verhindern. Bei Angriffen mehrerer mit Ransomware in Verbindung gebrachter Gruppierungen zeigte sich, dass Unternehmen mit klar definierten Regeln Angriffe in der Anfangsphase abwehren und gleichzeitig bewusst von Menschen gesteuerte Aktionen verhindern konnten.

Perimeter beurteilen:
Unternehmen müssen Perimetersysteme ermitteln und schützen, über die Angreifer in das Netzwerk eindringen können. Mit öffentlichen Scanschnittstellen wie RiskIQ können Daten erweitert werden.

Mit dem Internet verbundene Ressourcen besser schützen:
Insbesondere in der ersten Zugriffsphase nutzen Ransomware-Angreifer und Zugriffshändler ungepatchte Schwachstellen aus, ganz gleich, ob bereits bekannt oder noch unbekannt. Zudem nehmen sie schnell neue Schwachstellen ins Visier. Um das Risiko weiter zu minimieren, können Unternehmen die Funktionen für Bedrohungs- und Schwachstellenmanagement von Produkten zur Erkennung an Endpunkten und zur Abwehr nutzen und so Sicherheitslücken und Fehlkonfigurationen ermitteln und beseitigen.

Auf eine Wiederherstellung vorbereitet sein:
Eine optimale Ransomware-Abwehrstrategie sieht auch Pläne zu einer schnellen Wiederherstellung im Falle eines Angriffs vor. Es kostet weniger, die Systeme nach einem Angriff wiederherzustellen, als Lösegeld zu bezahlen. Achten Sie daher darauf, regelmäßige Sicherungen der kritischen Systeme anzufertigen und diese Sicherungen vor vorsätzlicher Löschung und Verschlüsselung zu schützen. Sofern möglich, sollten Sicherungen online in unveränderlichem Speicher oder komplett offline oder nicht vor Ort abgelegt werden.

Weitere Maßnahmen zur Abwehr von Ransomware-Angriffen

Die vielschichtige Bedrohung durch die neuesten Ransomware-Verfahren und die Schwierigkeit, von Menschen durchgeführte Ransomware-Angriffe zu stoppen, zwingt Unternehmen zu einer umfangreichen Sicherheitsstrategie.

Mit den oben aufgeführten Maßnahmen können Sie sich vor gängigen Angriffsmustern schützen und Ransomware-Angriffe weitgehend vermeiden. Damit Sie auch weiterhin vor herkömmlichen und von Menschen durchgeführten Ransomware-Angriffen und anderen Bedrohungen geschützt sind, nutzen Sie Sicherheitstools mit Funktionen zur domänenübergreifenden Transparenz und einheitlichen Untersuchung.

Eine weitere Übersicht über Ransomware inklusive Tipps und bewährten Vorgehensweisen zu Vermeidung, Erkennung und Schadensbehebung finden Sie im Artikel Schützen Sie Ihr Unternehmen vor Ransomware. Noch ausführlichere Infos zu von Menschen platzierter Ransomware gibt es im englischsprachigen Blog-Beitrag Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself von Senior Security Researcher Jessica Payne.

Aktuelle Informationen zu den neuen Sicherheitsproblemen finden Sie auf der Seite Security Insider.

Infografik weitergeben:

✉ f in 🐦

Microsoft