Acronis

WHITEPAPER

# Die fünf Phasen der Cyber-Immunität: **Acronis** Cyber Protect

Wie Gesundheits-maßnahmen auch unser digitales Wohlbefinden fördern können

Wenn man bedenkt, dass der menschliche Körper (je nach Schätzungen) etwa 30-100 Billionen Zellen und mindestens die gleiche Anzahl von Bakterienzellen enthält (wenn nicht mehr), dann ist es doch erstaunlich, dass ein derart komplexes System mit so vielen Eigenschaften so gut funktioniert. Diese Komplexität ist tatsächlich verblüffend.

Moderne Computersysteme sind im Vergleich zu biologischen Systemen wenig komplex. Typischerweise gibt es rund 40 Milliarden Prozessoreinheiten und ca. 10x so viele Speichereinheiten. Jedes dieser Elemente hat eine relativ einfache Struktur mit einer engen, spezifischen Funktion. Diese Strukturen sind darauf optimiert, ihre Funktionen mit Milliarden Zyklen pro Sekunde zu erfüllen (im Gegensatz zu menschlichen Neuronen, die mit ca. 200 Zyklen pro Sekunde feuern). Trotz dieser relativ einfachen Strukturen können Computer dank dieser Elemente schnell und über große Entfernungen miteinander kommunizieren – was jedoch ganz eigene, komplexe Herausforderungen schafft.

Dieses Whitepaper untersucht, wo es Gemeinsamkeiten zwischen biologischen und digitalen Bedrohungen gibt – und zeigt, wie Acronis Cyber Protect die einzigartigen Eigenschaften von Computersystemen nutzt, um ideale Antworten auf die modernen Risiken für Daten, Applikationen und Systeme zu liefern und MSPs so zu befähigen, ihre Kunden digital zu „immunisieren“ und #CyberFit zu machen.

# Die Ähnlichkeiten zwischen biologischen und digitalen Systemen

In der Vergangenheit gab es viele Fälle, in denen Computerviren versucht haben, ihren biologischen Namensgeber zu imitieren. Das Aids auslösende HI-Virus beispielweise greift zuerst das menschliche Immunsystem an und macht Menschen dadurch dann anfällig für weitere Krankheiten. Einige Malware-Varianten verfolgen einen ähnlichen Ansatz und deaktivieren zuerst das Antiviren-Tool eines Betriebssystems auf einem Computer, um so dessen Sicherheit insgesamt zu schwächen. Bekannte Beispiele dafür sind „Conflicker“ bei Windows oder „Shlayer“ bei MacOS.

Ein anderes raffiniertes Tool der Cyber-Kriminellen, „Double Agent“ genannt, kann eine Antiviren-Lösung selbst in eine Art Malware umwandeln, die dann wiederum das System angreift. Auf die biologische Ebene übertragen, würde dies einer Autoimmunerkrankung entsprechen, bei der die körpereigene Abwehr gesundes Gewebe angreift.

Und so, wie bestimmte biologische Erkrankungen durch schlechte Hygiene noch verschlimmert werden (wie beispielsweise jetzt bei der Corona-Pandemie), so gibt es auch „ungesunde“ Gewohnheiten in der digitalen Welt, durch die Cyber-Bedrohungen noch gefährlicher werden. Der Angriff durch die bekannte Ransomware „WannaCry“ hat sich nicht allein deswegen zu einer globalen Epidemie ausgeweitet, weil diese Ransomware besonders raffiniert gewesen wäre. Nein, vielmehr hatten die Angriffsopfer es versäumt, die durchaus verfügbaren Sicherheits-Patches aufzuspielen. Genau dies gehört aber zu den empfohlenen Vorgehensweisen (Best Practices) einer guten „Computer-Hygiene“.

Betrachtet man diese Ähnlichkeiten, so wird deutlich, wie wichtig die Früherkennung und Eindämmung von Krankheitserregern ist – was gleichermaßen für die körperliche und digitale Gesundheit gilt.

Wenn wir über weitere Möglichkeiten nachdenken, äußere Bedrohungen zu kontern, dann können wir aus dem Vergleich biologischer und digitialer Systeme noch mehr lernen. Denn in beiden Fällen lässt sich die Vorgehensweise in fünf Hauptphasen unterteilen: das Vermeiden, Erkennen, Reagieren, Beheben und Analysieren. Im Computerbereich sind folgende Begriffe üblicher: Prävention, Erkennung, Reaktion, Wiederherstellung und Forensik.


Copyright © 2002-2020 Acronis International GmbH.

# 1. Prävention

**Es gibt vier wesentliche Ansätze, um biologische Krankheiten zu vermeiden:**

- **Gesunde Lebensgewohnheiten**. Das heißt: gesund essen, schlafen, Sport treiben und Stress vermeiden. Diese Maßnahmen machen uns, insbesondere in Kombination, gesünder, stärker und widerstandsfähiger – wodurch wir Krankheiten besser abwehren können. Und auch regelmäßige Arztbesuche unterstützen unsere Gesundheit.
- **Gute Hygiene.** Einfache Handlungen wie Händewaschen, tägliches Duschen und Reinigen der Wohnung (insbesondere Küchen- und Badezimmeroberflächen), verringern das Infektionsrisiko, indem sie unnötige Expositionen durch schädliche Bakterien und Viren beseitigen.
- **Impfungen.** Wenn wir unseren Körper mit einem geschwächten, kontrollierten Stamm eines Krankheitserregers konfrontieren, können wir unser Immunsystem so trainieren, dass es wirksam reagieren kann, wenn es zukünftig auf den entsprechenden ungeschwächten Erreger treffen sollte.
- **Isolation.** In Umgebungen mit hohem Risiko kann das Tragen von persönlicher Schutzausrüstung (Masken, Kittel etc.) die Ausbreitung übertragbarer Krankheiten verhindern und gefährliche Erreger isolieren.

**Dieselben Ansätze können auch bei Computersystemen angewendet werden, um Schäden zu vermeiden:**

- **Gesunde Lebensgewohnheiten.** Ihr System regelmäßig zu analysieren und zu testen, erhöht dessen „Resilienz". Dazu gehört insbesondere das Identifizieren und Beheben möglicher Schwachstellen. Acronis Cyber Protect hält Ihre Systeme in guter Verfassung, indem es diese regelmäßig auf Schwachstellen prüft und die neuesten Patches installieren kann. Dazu gehört auch ein Selbstschutzmechanismus – analog zum Immunsystem eines Körpers. Dieser gewährleistet, dass die bereitgestellten Schutzfunktionen fortlaufend arbeiten und Sie #CyberFit bleiben.
- **Gute Hygiene**. So wie bei der körperlichen Hygiene einfache Maßnahmen (wie Händewaschen) entscheidend sind, müssen auch IT-Anwender lernen, bewährte Verfahren zur Infektionsvermeidung anzuwenden. Dazu gehören Empfehlungen wie keine dubiosen Programme herunterzuladen, keine fragwürdigen Websites aufzurufen und – insbesondere in E-Mails – nicht leichtgläubig auf Links zu klicken oder den Angaben von Fremden zu vertrauen, auch wenn diese sich als Freunde ausgeben sollten. Es ist zudem wichtig, Ihre Daten gut zu organisieren. Denn gut gesicherte und vor Kompromittierung geschützte Daten können nutzlos werden, wenn Sie nicht mehr wissen, wie Sie auf diese zugreifen können. Es ist außerdem entscheidend, ein regelmäßiges Backup durchzuführen!

  Und so wie ein Arzt Sie auf Gesundheitsgefahren hinweisen kann, so können Sie auch auf dem Computer „gesund" bleiben, wenn Sie stets gut informiert sind und vor neuen Gefahren gewarnt werden. Unser globales Netzwerk der Acronis Cyber Protection Operation Centers (CPOCs) stellt intelligente Alarmmeldungen bereit, um IT-Abteilungen über neue Gefahren zu informieren. Mithilfe intelligenter Schutzpläne, die auf diese Alarmmeldungen reagieren können, lässt sich so der Schutz und die Sicherung der Daten automatisch das jeweilige Risikoniveau anpassen.
- **Impfungen.** Während bestimmte Programme die „Abwehrkräfte" Ihres Systems stärken können, entspricht Acronis Cyber Protect eher einem richtigen „Immunsystem" für Ihren Computer. Wie das biologische Gegenstück erkennt und neutralisiert es gefährliche „Fremdstoffe" (in der Biologie „Antigene" genannt) in Ihrem System, bevor diese nennenswerte Schäden anrichten können. Denn Acronis Cyber Protect verfügt über integrierte Abwehrmechanismen, welche wiederum auf Regeln basieren, die von der Acronis Cyber Engine bereitgestellt werden. Da diese Engine als gemeinsame Abwehrbasis für alle geschützten Computer dient, profitieren diese unmittelbar alle davon, wenn die Engine eine neue Malware per „Machine Learning" erfasst. So kann die Engine eine Immunität gegen neue Bedrohungen aufbauen und diese – wie über einen Impfstoff – allen Computern bereitstellen.
- **Isolation.** Um in Systeme eindringende Schadprogramme bzw. „bösartige Agenten" zu isolieren und die Systeme vor Schäden zu bewahren, wurden verschiedene Techniken wie Sandboxen, Container, Netzwerk-Firewalls, Angriffsverteidigungssysteme (IPS, Intrusion-Prevention-Systeme) und Netzwerkfilter entwickelt.


Copyright © 2002-2020 Acronis International GmbH.

# 2. Erkennung

Unser Körper erkennt Krankheitserreger, indem er Bakterien oder Viren auf bestimmte Merkmale hin „scannt", die dann als „körpereigen" oder „fremd" eingestuft werden. Cytotoxische T-Zellen beispielsweise können Fremdkörper/Eindringlinge als gefährlich kennzeichnen und so das weitere Immunsystem aktivieren, um den Erregerangriff abzuwehren.

Biochemische Erkennungsprozesse sind hochkomplex und können manchmal sogar aus dem Ruder laufen. Etwa infolge von Fehlerkennungen oder Kreuzreaktionen, weil (auch) körpereigene Strukturen als Antigene erkannt werden. Das kann zu überschießenden Immunreaktionen oder sogar Autoimmunerkrankungen führen, bei denen der Körper sich dann selbst angreift. Solche Autoimmunerkrankungen sind zwar relativ selten, können aber extrem gefährlich sein.

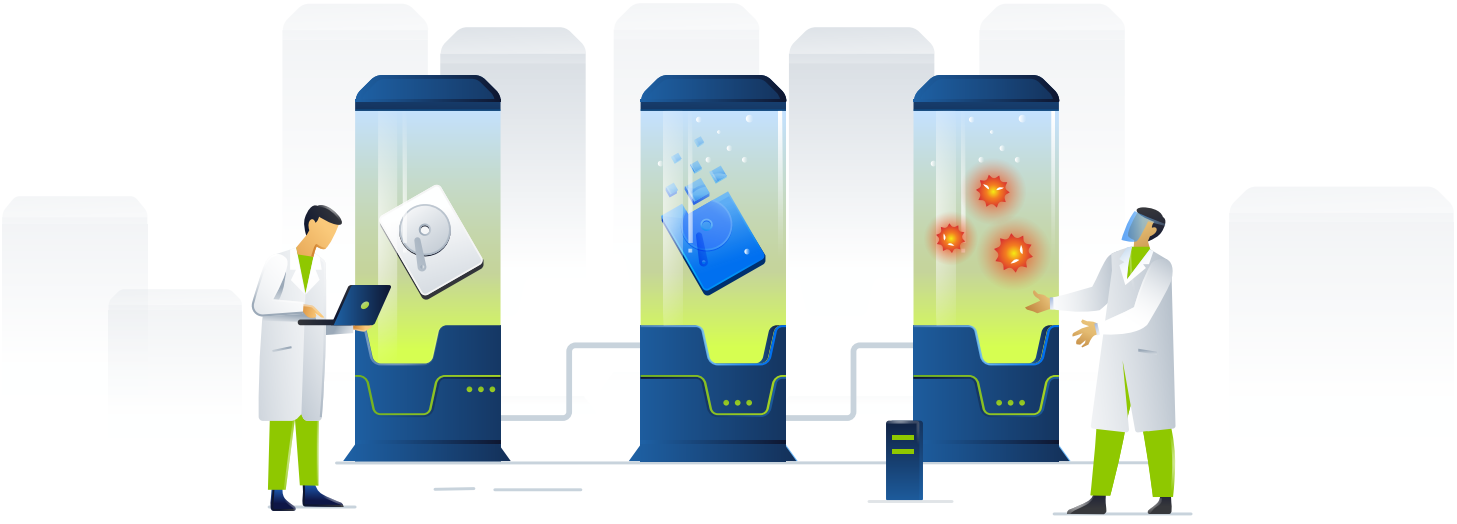
Ähnlich dem körpereigenen Erkennungssystem können auch Ärzte ihre Patienten auf Erkennungszeichen untersuchen – beispielsweise einfache Symptome wie Fieber und Husten. Genauere, zeitaufwendigere Tests können dann über Antikörper, Antigene oder genetisches Material (DNA/RNA) den Erreger nachweisen.

Die gute Nachricht in Bezug auf Computersysteme ist, dass diese meistens einfacher zu untersuchen sind als der menschliche Körper. Wann immer ein Computerprogramm etwas tun will, muss es mit anderen Systemkomponenten interagieren, beispielsweise Systemdienste oder APIs aufrufen. Das heißt, dass es seine Aktionen nie ganz verbergen kann – weswegen auch bösartige Programme auffindbar sind.

Weil Acronis Cyber Protect auf der Acronis Cyber Engine basiert, kann es alle Applikationen und Benutzer konstant auf verdächtige Aktivitäten überwachen. Dabei ist es auch in der Lage, neue heuristische Regeln zur Erkennung böswilliger Verhaltensmuster zu entwickeln. Und zwar sowohl eigenständig als auch durch zusätzliche Informationen von Cyber-Analysten.

Die Cyber Engine kann insbesondere die Anwesenheit eines bösartigen Programmcodes auf einem Computer erkennen (selbst wenn dieser Code so entwickelt wurde, dass er sich als Bestandteil einer zulässigen Applikation ausgibt und so zu verstecken sucht) – oder einen Cyber-Kriminellen melden, der mithilfe gültiger, aber gestohlener Anmeldedaten ins System eingedrungen ist. Ein Beispiel: wenn Microsoft Word auf einmal die APIs zum Lesen/Schreiben von Dateien häufiger als üblich aufruft oder Daten von einer Website herunterlädt, die zuvor noch nie besucht wurde, so wird dieses Verhalten sofort erkannt und als verdächtig gekennzeichnet.

Und Acronis Cyber Protect lernt, wie ein guter Doktor, ständig dazu – eigenständig, auf der Basis gespeicherter Kenntnisse oder mithilfe von Analysten und Partnern, die entsprechende Informationen liefern. Auf diese Weise kann Acronis Cyber Protect Infektionen schneller und zuverlässiger erkennen als so manches biologisches System – mit weniger falsch-positiven bzw. negativen Ergebnissen.




Copyright © 2002-2020 Acronis International GmbH.

# 3. Reaktion

Sobald eine Bedrohung erkannt wird, mobilisiert das Immunsystem eines Körpers seine „Truppen", um die Bedrohung zu beseitigen. Wir können die Reaktionen unseres Körpers auf eine Infektion in Form von Entzündungen, Fieber und anderen, oft unangenehmen Symptomen erleben, während unsere Immunabwehr den Erreger bekämpft.

Allerdings kann es etwas dauern, bis der Körper die angemessene Reaktion auf eine Infektion gefunden hat. Beispielsweise müssen manche Signale zu den Lymphknoten geleitet werden, um die Reaktion des Körpers zu unterstützen. Nur durch das richtige Zusammenspiel kann der Körper effektiv auf Infektionen reagieren.

Auch wenn unser Körper eine Infektion vielleicht recht früh erkennt, werden wir selbst des Problems meist erst dann bewusst, wenn wir eine spürbare Reaktion (wie Fieber, Lymphknotenschwellung etc.) unseres Körpers erleben. Wenn sich solche Symptome bemerkbar machen, kann man zum Arzt gehen, um eine Diagnose und/oder ggf. Medikamente zu erhalten, die die Symptome lindern oder die Genesung beschleunigen.

Der gleiche Ansatz kann auch auf Computersysteme übertragen werden. Sobald eine digitale Bedrohung erkannt wird, kann Acronis Cyber Protect schnell über geeignete Gegenmaßnahmen entscheiden. Die MSPs und MSSP-Partner von Acronis können währenddessen die Systeme mit Acronis Cyber Protect weiter überwachen und wertvolle Erkenntnisse liefern, um die Acronis Cyber Engine weiter zu verbessern. Diese IT-Profis sind wie ein perfekter Hausarzt, der Ihren Gesundheitszustand fortlaufend in Echtzeit überwacht und bei einer Infektion umgehend reagiert. Was natürlich deutlich schneller und besser ist, als drei Tage zu warten, um zu sehen, ob die Krankheitssymptome nicht von alleine weggehen.

Damit ist gemeint: egal ob in der biologischen oder digitalen Welt – je früher man reagiert, desto geringer der Schaden und umso schneller die Wiederherstellung.

# 4. Wiederherstellung

Die Überwindung einer Infektion und die Wiederherstellung von geschädigten Zellen bzw. Gewebe kann langsam und belastend sein: selbst eine gewöhnliche Erkältung verläuft oft über mehrere Tage. Viele Infektionen ist schwerwiegender – und dann benötigt unser Körper oft Hilfe, um diese abzuwehren.

Medikamente (wie Antibiotika, Virostatika, Entzündungshemmer), medizinische Überwachungen oder im Extremfall Krankenhausbehandlungen können teuer und zeitaufwendig sein.

Wenn es jedoch um die Wiederherstellung von Cyber-Angriffen geht, verfügt Acronis Cyber Protect über einzigartige Fähigkeiten, die auf der engen Integration mit seiner Backup-Funktionalität beruhen. Denn damit können Sie Systeme jederzeit auf den letzten bekannten „gesunden Zustand" zurückversetzen – und zwar **ohne jeden Datenverlust.** Dabei können möglicherweise doch im Backup eingebettete Bedrohungen (wie versteckte Malware) automatisch erkannt und fehlende Patches auf das wiederhergestellte System angewendet werden. Dadurch wird vermieden, dass dieselbe Bedrohung im wiederhergestellten System erneut zu Problemen führt.

Acronis Cyber Protect tritt umgehend in Aktion, noch bevor der MSP oder MSSP alarmiert wird, der das betroffene System verwaltet. Acronis Cyber Protect versucht zuerst, den entsprechenden Schadcode aus dem System zu entfernen (sofern möglich oder praktikabel). Anschließend versucht es, die Auswirkungen des Angriffs soweit wie möglich zu mindern. Bei besonders komplexen Fällen (etwa, wenn es schwierig ist, sich für eine automatisierte Aktion zu entscheiden) alarmiert Acronis Cyber Protect den entsprechenden Systemadministrator. Dieser kann dann per Fernwartung (Remote Desktop-Funktionalität) sicher auf das System zugreifen.


Copyright © 2002-2020 Acronis International GmbH.

# 5. Forensik

Bei körperlichen Erkrankungen denken wir selten an die forensische Maßnahmen, die bei Bekämpfung helfen könnten. Die Arbeit von Forschern zum Verstehen, Behandeln oder gar Ausrotten von Krankheiten bleibt daher oft unbeachtet. Doch solche forensischen Untersuchungen spielen auch eine wichtige Rolle, um uns zukünftig vor biologischen wie auch digitalen Bedrohungen zu schützen.

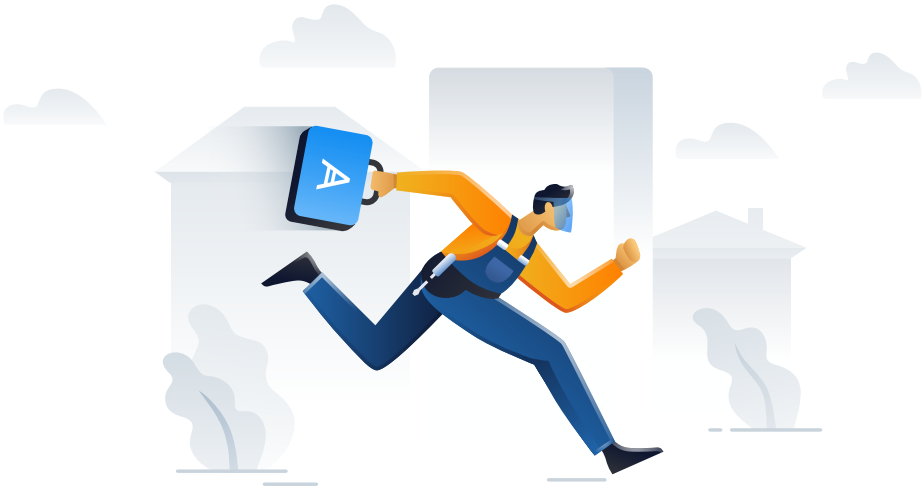
Bitte beachten Sie: Wir würden wohl immer noch unter vielen schlimmen Krankheiten (wie der Pest oder den Pocken) leiden, wenn Wissenschaftler diese Krankheiten nicht zu ihren Ursprüngen zurückverfolgt, die „Brutstätten" für die Erreger beseitigt und wirksame Impfstoffe sowie genetische Verfahren (wie Sequenzierungen) zur Bekämpfung solcher Krankheiten entwickelt hätten.

Bei Epidemien bzw. Pandemien ist es üblich, die Ausbreitung der Krankheit einzudämmen, indem die Kontakte von infizierten Personen verfolgt und Quarantäne-Maßnahmen umgesetzt werden. Außerdem sollten die betreffenden Personen diagnostiziert und ggf. behandelt werden.

Eine ähnliche forensische Arbeit spielt auch in der digitalen Welt eine wichtige Rolle. Acronis sammelt weltweit Signale von allen durch unsere Software geschützten Endpunkten, die das CPOC-Team auf neue Bedrohungen überwacht. Sobald eine neue Bedrohung identifiziert wird, analysiert das Team den Quellcode, um Gegenmaßnahmen zu entwickeln. Wenn unseren Analysten spezielle Backups mit forensischen Daten zur Verfügung gestellt werden, können Sie einen Angriff schnell und präzise untersuchen, um beispielsweise dessen Ursprung zu ermitteln. Mit dieser Fähigkeit kann Acronis Cyber Protect diejenigen Informationen bereitstellen, die benötigt werden, um das betreffende System schnell und ohne Datenverlust zu „heilen".

# Partnerschaft mit MSPs und MSSPs

So wie wir uns in puncto Gesundheit auf medizinische Experten verlassen, so vertraut Acronis auf seine MSP- und MSSP-Partner, damit unsere Kunden #CyberFit bleiben und mit „gesunden" Systemen arbeiten können. Die Zusammenarbeit mit einem MSP oder MSSP, der Acronis Cyber Protect einsetzt, ist der beste Weg, damit Ihre IT-Infrastruktur das gleiche Maß an Betreuung erhält wie Sie von Ihrem Hausarzt. So können Ihre Systeme fortlaufend überwacht und deren Schutz von hochqualifizierten Mitarbeitern betreut werden. Diese halten Ihre IT-Umgebung sauber und sorgen für eine gute „Hygiene", um das Infektionsrisiko zu minimieren. Sollte es dann doch einmal zu einem Desaster kommen, können Sie direkt auf die Hilfe von Experten zurückgreifen.



Acronis

Weitere Informationen erhalten Sie unter
**www.acronis.com**

Copyright © 2002-2020 Acronis International GmbH. Alle Rechte vorbehalten. Acronis und das Acronis Logo sind eingetragene Markenzeichen der Acronis International GmbH, in den Vereinigten Staaten und/oder in anderen Ländern. Alle anderen Marken oder eingetragenen Marken sind das Eigentum ihrer jeweiligen Inhaber. Technische Änderungen, Abweichungen bei den Abbildungen sowie Irrtümer sind vorbehalten. 2020-05