Z! DAS ZUKUNFTSMAGAZIN IM INTERVIEW MIT REINALD KEMPF

Reinald Kempf, Geschäftsführer der echoway GmbH

Die Zahlen vom BSI sind eindeutig. Cyber Crime Aktivitäten nehmen ständig zu, die Bedrohungslage ist eine große Herausforderung für Unternehmen jeder Größe und Branche. Reinald Kempf ist seit vielen Jahren als Experte für Informationssicherheit Ansprechpartner für Unternehmen in der Region. Im Gespräch mit Z! Das Zukunftsmagazin erklärt er, was sich in den letzten Jahren verändert hat und worauf IT-Administratoren achten sollten.

Z! In der aktuellen Ausgabe des Zukunftsmagazins ist der Schwerpunkt IT-Sicherheit. Das ist doch nichts Neues, oder?
Natürlich war das schon immer in den Unternehmen ein wichtiger Punkt, sich um die Sicherheit der Daten und IT-Systeme zu kümmern. Doch die Rahmenbedingungen waren früher ganz andere, weswegen das Thema schon sehr heiß ist. Denken Sie an die jüngsten Medienberichte mit lahmgelegten Servern, erpressten Geldern und manipulierten Prozessen.

Z! Was hat sich also konkret an der Ausganglage in den letzten Jahren verändert?
Mehr als 25 Jahre gab es eine klassische Referenzinfrastruktur mit definierten Perimetern in der IT-Sicherheit. Diese war gekennzeichnet von einem zentralen Ausgang in das Internet, geschützt durch Firewall, DMZ inkl. Proxies, Serverdiensten, Portalen usw. Die Anbindung von Außenstellen erfolgte via VPN ohne lokalen Zugang zum Internet. Es gab nur wenige mobile MitarbeiterInnen, meist reduziert auf Vertrieb, Servicetechnik, Führungsebene. In der Regel gab es keine Cloud, bestenfalls Outsourcing oder Rechenzentrumsbetrieb z. B. von SAP im externen Rechenzentrum. Daher war auch eine Absicherung der Produktion nicht nötig. Office-IT und Operational-IT (OT) waren vielfach getrennt. Oft gab es nur eine Multifaktor- bzw. Einmalkennwort-Authentisierung für Administratoren, handverlesene MitarbeiterInnen bzw. Führungsebene oder flächendeckende, statische, schlechte Kennwörter.

Z! Und was ist jetzt anders?
Schauen Sie sich die Aufzählung von oben nochmal genau an. Was davon gilt heute noch für moderne IT-Architekturen? Die letzten Jahre und vor allem die Pandemie haben zu massiven Veränderung der Arbeitsweisen geführt. Da ist einiges in der IT in Bewegung, doch leider haben viele im Bereich der IT-Sicherheit der Dynamik nicht folgen können oder die neue Bedrohungslage nicht erkannt.

Z! Welche Rolle spielt aus Ihrer Sicht der Wechsel „in die Cloud“?
Der seit Jahren wachsende Cloud-Trend ist ein Treiber für einen radikalen Paradigmenwechsel auch für die IT-Sicherheit. Früher wurden einzelne Anwendungen (SAP, MRP, ERP, Datenbanken usw.) in „privaten“ Rechenzentren von Dienstleistern betrieben. Heute werden bei vielen Unternehmen mit einer „Cloud-First“-Strategie so schnell und viel wie möglich alle Arten von Servern (IaaS), Plattformen (PaaS) oder Diensten und Anwendungen (SaaS) außer Haus in die Public Cloud migriert. Allen voran Microsoft Azure und O365 oder AWS.

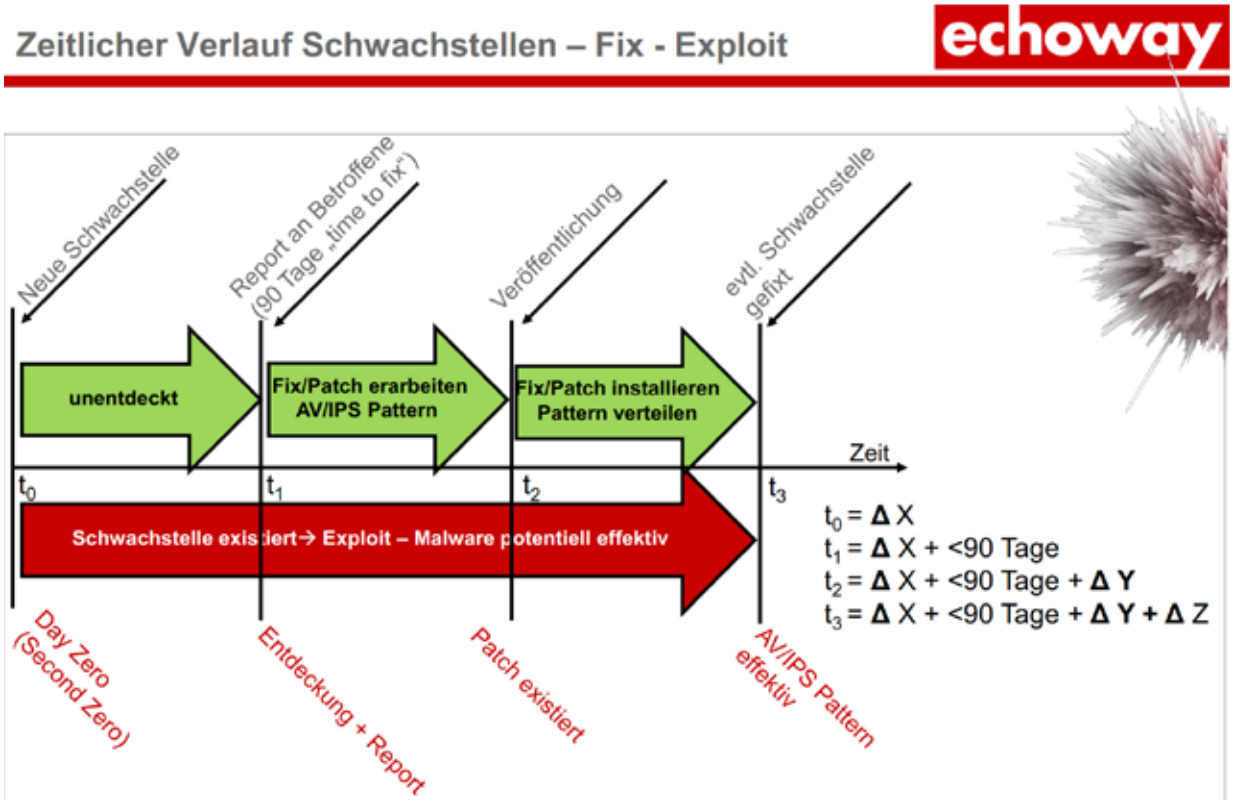
Neben datenschutzrechtlichen Herausforderungen (z. B. USA „Cloud Act“ vs. DSGVO) wird nun der eingangs beschriebene Architekturansatz massiv verändert. Unverschlüsselte (extern disponierte) Inhalte und WAN-Verbindungen (z. B. MPLS) sind hier zudem oft anzutreffen. Der Perimeter ist im Gegensatz zum früheren zentralistischen Ansatz „On Premises“ plötzlich überall: Cloud, mobile Endgeräte und Mobilität inkl. Privatnutzung, Öffnung der OT in der Produktion durch Industrie 4.0 und anderer Trends, Datenzugriff von überall auf wichtige IT-Bereiche rund um die Uhr.

Z! Und dann kam mit Corona auch noch Home Office im großen Stil.
Ja, genau. Anfangs, ab März 2020 ging es erst mal darum, die Belegschaft überhaupt irgendwie zu Hause „arbeitsfähig“ zu bekommen. Verständlich. Fatalerweise wurde das Sicherheitskonzept reziprok zur sich entwickelnden Bedrohungslage auf Dauer aufgeweicht oder im Klartext „die Augen zugedrückt“ und gehofft, dass nichts passiert. Typische Probleme waren und sind: Mangelnde Bandbreite des zentralen Zugangs ins Internet (inkl. Firewall, DMZ usw.), durch den sich nun manchmal statt 10 % wie früher, 90 % der Belegschaft via VPN erst mal eingewählt und dann entweder auf Unternehmensressourcen zugegriffen hat oder via besagter FW/DMZ/Proxy Infrastruktur ins Internet ging. Dazu kommt der Mangel an Hardware-Geräten wie PCs, Laptop etc. So wurden ja teilweise völlig unkontrollierte Privatrechner für den Zugriff auf Unternehmensressourcen verwendet!

Z! Was sind die Konsequenzen?
Die Unternehmen sind leicht verwundbar. Die Endpoint-PCs und Netze sind oft (auch heute noch) völlig unzureichend oder gar nicht geschützt. Eine Ransomware kann so bei der nächsten Einwahl per VPN zum Einfallstor werden und einen Flächenbrand auslösen. Die IT-Administratoren haben oftmals nur mangelhaften Überblick über das, was auf ihren Servern geschieht, da sie keine geeignete Sicherheitssoftware, beispielsweise SIEM, NDR, EDR, XDR etc. nutzen und können bei Problemen nicht rechtzeitig eingreifen.
Leider haben wir das in der Praxis alles vielfach sehen müssen und Unternehmen mit 2000 Mitarbeiter waren zwei Wochen komplett ohne IT inkl. (VoIP)-Telefonie. Da funktionierten bestenfalls noch das Handy und das Fax-Gerät!

Z! Was sagen Sie zu Leuten, die meinen: „Wir haben doch Firewalls und überall einen Virenscanner installiert“?
Einfache Antwort: Das reicht nicht! Mit Ransomware wie Locky wurde im Februar 2016 ein neues Zeitalter einberufen. Nein, Malware dieser Art war nichts Neues. Eindrucksvoll hat Stuxnet 2010 der Welt schon demonstriert, wie man in diesem Fall die Anreicherungsanlagen im Iran mit neuen „Cyberwaffen“ kontrolliert bzw. destruiert. Neu mit Locky ist nur die Tatsache, dass nun neben Wirtschaftsspionage und staatlich motivierten Cyberangriffen das kommerzielle Zeitalter von Malware eingeläutet wurde. Ein Milliardengeschäft mit Ransomware und erpressten Geldern. Der Trend wird erheblich zunehmen, denn im Gegensatz zu „klassischem“ Terrain wie Drogenhandel, Prostitution etc. ist man aufgrund der physischen „Absenz“ im Ausland im Prinzip geschützt vor Strafverfolgung.

Z! Politische Krisen bringen immer auch Cyber-Kriminelle auf den Plan. In Pandemiezeiten wurde von „umgeleiteten“ Fördermitteln berichtet. Was hört man zum Ukraine-Konflikt?
Der aktuelle Ukraine-Konflikt feuert nun die bereits hinreichend bekannte, regierungsmotivierte und -gestützte Hacking-Aktivität massiv an. Parallel wird sich die kriminelle Schattenwelt, zu der auch maßgeblich russische Banden gehören, auf die neue Situation stürzen. Z. B. durch gehackte impersonifizierte Accounts oder Postfächer von Mitarbeitenden, Partnern, Kunden, Zulieferern deutscher Unternehmen. Hier scheitern dann oftmals jegliche „Awareness-Maßnahmen“ für die Mitarbeiter, wenn aus bisher vertrauenswürdigen Kommunikationsbeziehungen bzw. Quellen nun „böse“ Dateianhänge, Links oder Phishing-Mails (und Anrufe) im Tagesgeschäft einfließen. Auch in der Personalabteilung scheitert die Vorgabe „bitte nur Anhänge von E-Mails von bekannten/vertrauenswürdigen AbsenderInnen annehmen!“ BewerberInnen sind in der Regel immer unbekannt!



Z! Wo liegt der Ursprung für mobile Malicious Code?
Vorläufer von Locky, Emotet & Co. gibt es grundsätzlich schon seit 25 Jahren, seit es Java und Active X auf Webseiten gibt. In den 1990er Jahren hat man erkannt, dass man durch Webdienste via Browser auch auf lokale Ressourcen auf dem PC (Registry, Dateisystem, Prozesse usw.) über z. B. eine Webseite/ein Portal zugreifen kann. Der Wegbereiter aller heutigen Web-Applikationen.

Z! Man hört oft von Sicherheitslücken und dass diese geschlossen werden müssen.
Patchen, sprich, das Schließen von Sicherheitslücken, ist natürlich wichtig. Aber was nutzt ein Patch, wenn die Schwachstelle schon Monate (siehe Abbildung) vorher im Darknet ausgenutzt wird, bevor diese das erste Mal von einem „ethical Hacker" oder Anwender z. B. an Microsoft, Adobe oder Apple reportet wird. Selbst dann muss es erst noch einen Patch geben und dieser muss dann noch ausgerollt und installiert sein. Das Einfallstor besteht dann über einen sehr langen Zeitraum, in welchem die besagten „alten" Technologien absolut blind sind und keine Abwehr bieten. Es ist eben „unbekannte" Malware. Log4j war hier Ende 2021 ein lehrhaftes, eindrückliches Beispiel. Viele Systeme dürften heute noch anfällig sein.

Z! Welche Technologien zur Abwehr sollte jeder IT-Administrator aus Ihrer Sicht kennen?
Aus meiner Erfahrung gibt es da tatsächlich Nachholbedarf und Wissenslücken. Generell kann man die Technologien zur Malwarebekämpfung grob in zwei Klassen einteilen: Einmal die Abwehr bekannter Malware: klassische „Threat Prevention" Anti-Spam, Antivirus, Intrusion Prevention usw. Die Technologie leistete etwa drei Jahrzehnte gute Dienste, ist aber heute bestenfalls noch für die schnelle Vorerkennung/Filterung hilfreich. Wichtiger sind also die Technologien zur Abwehr unbekannter Malware (Zero Day, Zero Second). Dazu zählen NDR, EDR, Sandboxing, CPU Level Inspection, Link Analyse und Prefetch, Content Disarm & Reconstruction bzw. Passivieren von Dokumenten. Damit werden aus z. B. aktiven E-Mail-Attachments wie PDF, XLS, DOC mit Macros bei der Erstzustellung passive Versionen ohne jegliches Gefährdungspotenzial. Natürlich kann ergänzend auch der Einsatz von Künstlicher Intelligenz helfen. Diese Dienste müsste man nun an allen oben genannten Perimetern vorschalten. Die Realität ist leider oft, dass bestenfalls der lokale Virenscanner noch den einzigen bzw. letzten Rettungsanker darstellt.

Z! Der IT-Administrator steht vor einer Vielzahl an Produkten und Anbietern. Wie kann er sich informieren?
Das ist in der Tat eine Herausforderung. Tatsächlich haben fast alle Anbieter solcher Sicherheitslösungen unterschiedliche Implementierungsformen und Pakete zu unterschiedlichen Kosten. Es ist aber nicht bekannt, warum diese mehr kosten und was sie dann genau mehr leisten, eben z. B. den essenziellen Schutz vor unbekannter Malware. Da ist der Markt mit vielen Schlagworten unübersichtlich, aber vor allem das Know-how auch in erfahrenen IT-Teams nicht tiefgreifend genug.

Wir bei Echoway schauen uns die Systeme unserer Kunden an und rüsten bei Bedarf nach: an der Firewall On Premises, in der Cloud (IaaS, SaaS, Container ...), auf den Endpoints, in der Mailkette, auf Servern, im Netzwerk ...

Dass dies ein lohnender Aufwand ist, zeigt z. B. die MITRE-ATT&CK Evaluation, die auf absolut neutralem Boden Virenscanner (oder besser Endpoint-Sicherheitsprodukte) auf „Herz und Nieren" – offen und transparent dokumentiert und gegen bekannte Herangehensweise auf Abwehrfähigkeiten unbekannter Malware prüft. [1]

Z! Nochmal im Klartext, was kann man tun für die eigene IT-Sicherheit?
Die wichtigsten Punkte sehe ich hier in der präventiven Abwehr von unbekannter Malware an allen Perimetern: On Premises, Cloud, Home Office, Produktion, Lokationen... Weiterhin die Überwachung des Netzwerkes bzw. Datenverkehrs, Echtzeitforensik, Incidence Response sowie die Konsolidierung von Lösungen, um möglichst viel Daten für intelligente (AI basierte, oder auch menschliche) Forensikanalysen und daraus abgeleitet Abwehraktivitäten in einem Guss zu haben. Auf die IT-Sicherheit zahlen sich weiterhin eine starke Authentisierung, Verschlüsselungstechnologien und die Bewusstseinsschulung der Mitarbeitenden aus.

Z! Nun passieren ja die Sachen immer bei den „Anderen" und im eigenen Haus gibt es diese Probleme nicht.
Guter Punkt. Aber seien Sie sich nicht zu sicher. Da läuft mehr im Verborgenen als man denkt. Es sind nicht nur die vielen sichtbaren Ransomsoftware-Angriffe relevant, bei denen Lösegeld von Unternehmen und Organisationen gefordert werden. Der Spionage- oder Betrugstrojaner unternimmt alles, um so lange wie möglich (siehe Beispiel Stuxnet) oder für immer unentdeckt zu bleiben.

Z! Wie kann man herausfinden, wie hoch die Bedrohungslage ist?
Wir analysieren das gerne mit z. B. einem Zero Day Malware Audit, oft zunächst in der Mailkette, und zeigen die „Funde" mit geeigneter Technologie, die vor dem Eingang z. B. des Exchange Servers ankommen. Die Ausgangslage ist ja die Annahme, dass durch Firewall, Threat Prevention, Proxy, E-Mail Gateway, Antispam, IPS usw. kein „böser" Anhang, Link etc. noch ankommt. Doch siehe da:
Keiner unserer (sehr sehr vielen) Audits hat in der Testphase von vier Wochen ein Ende gefunden, ohne einen gefährlichen, unbekannten Schädling zu finden und bei eingeschaltetem Prevention Modus zu eliminieren! Der Aufwand für ein solches Testat ist i.d.R. sehr überschaubar und kein Hinderungsgrund. Das Problem betrifft alle Branchen, alle Unternehmensgrößen, sprich jeden!

Vielen Dank, Herr Kempf für die interessanten Ausführungen und weiterhin viel Erfolg beim Kampf für mehr IT-Sicherheit.

Das Interview führte Katja Leimeister, approdos consulting.

Ansprechpartner

Reinald Kempf
echoway GmbH
Industriering 7
63868 Großwallstadt
06022 50872-0
info@echoway.de
www.echoway.de

1 Über die MITRE-ATT&CK EVALUATION können Sie sich unter den folgenden Links informieren: https://attack.mitre.org/matrices/enterprise/ und https://attackevals.mitre-engenuity.org/enterprise/participants/?adversaries=carbanak_fin7